

RECORD OF TRIAL²

of

(Station or Ship)

By

COURT-MARTIAL

Convened by _____ Commander _____

(Title of Convening Authority)

(Unit/Command of Convening Authority)

Tried at

(Place or Places of Trial)

(Date or Dates of Trial)

Date or Dates of Trial:

23 February 2012, 15-16 March 2012, 24-26 April 2012, 6-8 June 2012, 25 June 2012, 16-19 July 2012, 28-30 August 2012, 2 October 2012, 12 October 2012, 17-18 October 2012, 7-8 November 2012, 27 November - 2 December 2012, 5-7 December 2012, 10-11 December 2012, 8-9 January 2013, 16 January 2013, 26 February - 1 March 2013, 8 March 2013, 10 April 2013, 7-8 May 2013, 21 May 2013, 3-5 June 2013, 10-12 June 2013, 17-18 June 2013, 25-28 June 2013, 1-2 July 2013, 8-10 July 2013, 15 July 2013, 18-19 July 2013, 25-26 July 2013, 28 July - 2 August 2013, 5-9 August 2013, 12-14 August 2013, 16 August 2013, and 19-21 August 2013.

1 Insert "verbatim" or "summarized" as appropriate. (This form will be used by the Army and Navy for verbatim records of trial only.)

2. See inside back cover for instructions as to preparation and arrangement.

(A) 29 March 2012/2 April 2012/12 April 2012/17 April 12 – defense notifications and redactions

(B) 17 April 2012/19 April 2012 – Government Objections and Motions for Protective Order

(C) 20 April 2012 – Defense Replies

(15) Defense Motion to Reconsider Compel Discovery – Grand Jury (unscheduled)

c. Phase 2(b). Legal Motions, excluding Evidentiary Issues (10 May 2012 - 8 June 2012)

(1) Defense Motion to Dismiss All Charged Offenses under 18 U.S.C. 793(e)

(A) Filing: 10 May 2012

(B) Response: 24 May 2012

(C) Reply: 30 May 2012

(D) Article 39(a): 6-8 June 2012

(2) Defense Motion to Dismiss All Charged Offenses under 18 U.S.C. 1030(a)(1)

(A) Filing: 10 May 2012

(B) Response: 24 May 2012

(C) Reply: 30 May 2012

(D) Article 39(a): 6-8 June 2012

(3) Government Motion for Proposed Lesser Included Offenses

(A) Filing: 10 May 2012

(B) Response: 24 May 2012

(C) Reply: 30 May 2012

(D) Article 39(a): 6-8 June 2012

(4) Defense Proposed Lesser Included Offense Instructions

(A) Filing: 10 May 2012

(B) Response: 24 May 2012

(C) Reply: 30 May 2012

(D) Article 39(a): 6-8 June 2012

(5) Defense Motion to Exclude Uncharged Misconduct (MRE 404(b))

(A) Filing: 10 May 2012

(B) Response: 24 May 2012

(C) Reply: 30 May 2012

(D) Article 39(a): 6-8 June 2012

(6) Updated Proposed Case Calendar

(A) Filing: 10 May 2012

(B) Response: 24 May 2012

(C) Reply: 30 May 2012

(D) Article 39(a): 6-8 June 2012

(7) Disclosure of Unclassified Results of 3 Damage Assessment Searches to Defense in Response to the Court's Ruling, 30 March 2012

(A) Filing: 18 May 2012

(8) Disclosure under RCM 701(g)(2) or MRE 505(g)(2) of all Information (Unclassified and Classified) to the Court in Response to the Court's Ruling, 30 March 2012

(A) Filing: 18 May 2012

(9) Government Filing for In Camera Proceeding IAW MRE 505(i) with Notice to Defense (if Privilege is Claimed) in Response to the Court's Ruling, 30 March 2012

(A) Filing: 18 May 2012

(B) Response: 31 May 2012

(C) Reply: N/A

(D) Article 39(a): 6-8 June 2012

(10) Witness Lists Exchanged (Based on Discovery Received)

(A) Filing: 18 May 2012

(B) Government Objections: 24 May 2012

(C) Reply: 31 May 2012

(D) Article 39(a): 6-8 June 2012

(11) Production of Compelled Discovery #1 – Classified and Unclassified.

(A) 13 July 2012

d. Phase 3. Evidentiary Issues *not* Involving Classified Information under MRE 505 (22 June 2012 - 20 July 2012)

(1) Defense Motion to Compel Discovery #2

(A) Filing: 22 June 2012

(B) Response: 6 July 2012

(C) Reply: 11 July 2012

(D) Article 39(a): 18-20 July 2012

(2) Government Motion to Compel Discovery

(A) Filing: 22 June 2012

(B) Response: 6 July 2012

(C) Reply: 11 July 2012

(D) Article 39(a): 18-20 July 2012

(3) Motions *in Limine* (Evidence Discovered to Date)

(A) Filing: 22 June 2012

(B) Response: 6 July 2012

(C) Reply: 11 July 2012

(D) Article 39(a): 18-20 July 2012

- (4) **Motions to Suppress**
 - (A) Filing: 22 June 2012
 - (B) Response: 6 July 2012
 - (C) Reply: 11 July 2012
 - (D) Article 39(a): 18-20 July 2012

- (5) **Pre-Authenticate/Pre-Admit Evidence**
 - (A) Filing: 22 June 2012
 - (B) Response: 6 July 2012
 - (C) Reply: 11 July 2012
 - (D) Article 39(a): 18-20 July 2012

- (6) **Requests for Judicial Notice**
 - (A) Filing: 22 June 2012
 - (B) Response: 6 July 2012
 - (C) Reply: 11 July 2012
 - (D) Article 39(a): 18-20 July 2012

- (7) **Privileges**
 - (A) Filing: 22 June 2012
 - (B) Response: 6 July 2012
 - (C) Reply: 11 July 2012
 - (D) Article 39(a): 18-20 July 2012

- (8) **Proposed Members Instructions for all Charged Offenses**
 - (A) Filing: 22 June 2012¹
 - (B) Response: 6 July 2012
 - (C) Reply: 11 July 2012
 - (D) Article 39(a): 18-20 July 2012

- (9) **Compel Experts**
 - (A) Filing: 22 June 2012
 - (B) Response: 6 July 2012
 - (C) Reply: 11 July 2012
 - (D) Article 39(a): 18-20 July 2012

- (10) **Compel Witnesses**
 - (A) Filing: 22 June 2012
 - (B) Response: 6 July 2012
 - (C) Reply: 11 July 2012
 - (D) Article 39(a): 18-20 July 2012

¹ Since these instructions depend on the outcome of the motions to dismiss in Phase 2, the United States recommends scheduling this motion during Phase 3.

(11) Defense Notice of Intent to Disclose Classified Information under MRE 505(h)(1) (For Discovery Received)

(A) Filing: 22 June 2012²

(12) Article 13

(A) Filing: 15 June 2012³

(B) Response: 6 July 2012

(C) Reply: 11 July 2012

(D) Article 39(a): 18-20 July 2012

(13) Speedy Trial, including Article 10

(A) Filing: 15 June 2012⁴

(B) Response: 6 July 2012

(C) Reply: 11 July 2012

(D) Article 39(a): 18-20 July 2012

(14) Defense Notice of Plea/Forum

(A) Filing: 20 July 2012

e. Phase 4. Evidentiary Issues Involving Both Unclassified and Classified Information under MRE 505 (3 August 2012 – 4 September 2012)⁵

(1) Motions in Limine (Classified Information not Previously Disclosed)

(A) Filing: 3 August 2012

(B) Response: 17 August 2012

(C) Reply: 22 August 2012

(D) Article 39(a): 29-31 August 2012

(2) Motions to Suppress (Classified Information not Previously Disclosed)

(A) Filing: 3 August 2012

(B) Response: 17 August 2012

(C) Reply: 22 August 2012

(D) Article 39(a): 29-31 August 2012

² The defense should provide notice under MRE 505(h) when it files its witness list, so that the United States may start evaluating the list and more efficiently process the request through relevant Original Classification Authorities. If the privilege is required to be invoked, then this will provide the United States sufficient time to complete the necessary classification reviews, prior to Phase 4.

³ The filing date of one week earlier for the defense motions is in accordance with their schedule to give the United States the necessary time to respond.

⁴ The filing date of one week earlier for the defense motions is in accordance with their schedule to give the United States the necessary time to respond.

⁵ This process will likely require the military judge to review classified information within a special facility or under special handling procedures. Additionally, this process will likely take some time for the military judge to make her rulings on all classified information evidentiary motions.

(3) Pre-Qualify Experts

- (A) Filing: 3 August 2012
- (B) Response: 17 August 2012
- (C) Reply: 22 August 2012
- (D) Article 39(a): 29-30 August 2012

(4) Litigation Concerning MRE 505(h) and MRE 505(i)⁶

- (A) Filing: 3 August 2012
- (B) Response: 17 August 2012
- (C) Reply: 22 August 2012
- (D) Article 39(a): 29-31 August 2012

(5) Production of Compelled Discovery for Defense Motion to Compel Discovery #2 or Production of Limited Discovery under MRE 505(g)(2) or (3) or Notification to Court of Claim of Privilege under MRE 505(c)

- (A) Date: 17 August 2012

(6) Production of Compelled Discovery for Government Motion to Compel Discovery

- (A) Date: 3 August 2012

(7) Defense Additional Witness List in light of Information in Defense Motion to Compel Discovery. Defense Notice of Intent to Disclose Classified Information under MRE 505(h) from Compelled Discovery #2.

- (A) Date: 22 August 2012

(8) Proposed Questionnaires

- (A) Filing: 3 August 2012
- (B) Response: 17 August 2012
- (C) Reply: 22 August 2012
- (D) Article 39(a): 29-31 August 2012 (Questionnaires to members upon approval)
- (E) Completed Questionnaire Due Date: 14 September 2012.

f. Phase 5. Miscellaneous Motions (1 September 2012 – 21 September 2012)

(1) Any Additional Motion that does not have an Identified Deadline

- (A) Filing: 7 September 2012
- (B) Response: 14 September 2012
- (C) Article 39(a): 20 September 2012

(2) Grunden Hearing for all Classified Information

- (A) Filing: 7 September 2012
- (B) Response: 14 September 2012

⁶ Government advised the Court will need 15 duty days to review discoverable material.

(C) Article 39(a): 21 September 2012

(2) **Voir Dire Questions, Flyer, Findings/Sentence Worksheet**

(A) Filing for Court Review: 14 September 2012

(B) Article 39(a): 20 September 2012

h. **Phase 6. Trial by Members (20 September 2012 – 12 October 2012)**

(1) Article 39(a) Voir Dire – 20 September 2012

(2) Voir Dire: 21 September 2012

(3) Trial: 24 September 2012 – 12 October 2012

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, xxx-xx- [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

**DEFENSE REQUEST FOR
PARTIAL RECONSIDERATION
OF DISCOVERY RULING**

DATED: 12 April 2012

RELIEF SOUGHT

1. The Defense respectfully requests that the Court reconsider, in part, its ruling on the Defense Motion to Compel Discovery.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. As the moving party, the Defense has the burden of persuasion. R.C.M. 905(c)(2), 905(f). The burden of proof is by a preponderance of the evidence. R.C.M. 905(c)(1), 905(f).

ARGUMENT

3. In the Prosecution Response to Defense Motion to Compel Discovery ("Government Motion"), the Government stated the following:

The United States is in the process of producing all discovered information "relevant and necessary" to Defense's request that the United States has authority to disclose under federal rules. The United States disputes whether Defense provided a specific request, and adequate basis, for its request for "any grand jury testimony." However, in an abundance of caution, the United States intends to produce all grand jury materials, both classified and unclassified, that are "relevant and necessary" and that the United States has authority to disclose under the federal rules.

See Government Motion, p. 14. Presumably based on the Government's representation, the Court did not specifically address the grand jury testimony in its Ruling.

4. The Defense requested clarification from the Government on what exactly it intended to provide in regard to the grand jury materials. During an 802 telephonic conference, the Government seemed to suggest that it would produce all relevant material from the grand jury testimony. The Government explained that since there were some wholly irrelevant aspects to the grand jury testimony, those portions of the grand jury testimony would not be provided. The Government implied, however, that everything else would be provided. The Government indicated that it would provide such grand jury testimony in accordance with the timeframe established by the court (i.e. April 20).

5. Unfortunately, the Defense is still not clear on what exactly the Government was planning on turning over. On 9 April 2012, the Defense sent an email seeking further clarification. The email traffic reads as follows:

David Coombs: In your response to the Defense Motion to Compel Discovery, dated 8 March 2012, you stated “[t]he United States intends to produce all grand jury materials, both classified and unclassified, that are ‘relevant and necessary’ and the United States has authority to disclose under the federal rules.” During our last 802 conference you stated that you intended to provide the grand jury materials. Can you provide me with an estimated time line for these materials? Thank you.

Ashden Fein: We are working to review this material along with the FBI case file. If we find discoverable material, we will provide it to the defense as soon as possible once we confirm that we have the authority to disclose. We estimate that we will complete our review of any grand jury testimony in the next three weeks and intend to notify you of any discoverable material by 1 May. Additionally, we hope to disclose any discoverable material by 1 May as well.

David Coombs: I am not for sure I understand your response. What is the “discoverable material” standard that you are using to determine what to disclose? Also, why do you believe it would take until May 1st to complete your review? The Grand Jury investigation started in December of 2010. At that time, the Defense requested access to the investigation being conducted by the DOJ. Additionally, you have been on notice that these materials were the subject of a compel discovery motion since February. I am not clear on why the review hasn’t already been done, and why I don’t have these documents.

Ashden Fein: Material outside the possession of military authorities is discoverable under RCM 701(a)(6) and Brady. The United States has provided the defense FBI and grand jury material above and beyond this requirement and continues to review and coordinate additional review of material, including testimony. This case was referred in early February, and we have since been litigating this issue, which resulted in the United States informing the Court and defense that we intend to produce, as soon as practicable, any discoverable material we identify and have approval to make available. No later than 1 May is our best estimate considering the amount of information that the prosecution has a due diligence requirement to review and which we have been and are continuing to review.

David Coombs: Can you provide me with the Bates numbers for any grand jury testimony that have you provided to the Defense? Thank you.

Ashden Fein: We have not provided any grand jury testimony, only materials obtained through the grand jury.

6. In the Defense's opinion, it is still not clear what the Government will provide in relation to the grand jury materials. However, it seems based on the latest representations of the Government that not all relevant materials will be turned over. It only intends to disclose to the Defense *Brady* material under R.C.M. 701(a)(6).

7. Consequently, the Defense requests that the Court order the entire grand jury proceedings in relation to PFC Manning or Wikileaks to be produced to the Defense. Alternatively, the Defense requests that the grand jury proceedings be produced for *in camera* review to determine whether the evidence is discoverable under R.C.M. 701(a)(2) as being material to the preparation of the defense.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'DE Coombs', written over a horizontal line.

DAVID EDWARD COOMBS
Civilian Defense Counsel

11 April 2012

MEMORANDUM FOR RECORD

SUBJECT: Security Expert Review of Defense Motions

1. I hereby certify that I have reviewed the following Defense motions for the presence of classified information:

- a) Defense Response Motion to Prosecution's Motion to Preclude Reference to Actual Harm or Damage ; and
- b) Defense Request for Partial Reconsideration of Discovery Ruling;

I do not believe that either of these motions contains classified information or information that a reasonable person could believe to be classified.

2. The point of contact for this memorandum is the undersigned at (443) 861-9673.



CHARLES J. GANIEL
Command, SSO
HQ ATEC G-2/3/7

From: David Coombs
To: Lind, Denise R COL MIL USA OTJAG; Williams, Patricia CIV JFHO-NCR/MDW SJA; Jefferson, DaShawn MSG MIL USA OTJAG
Cc: Fein, Ashden MAJ USA JFHO-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHO-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHO-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHO-NCR/MDW SJA; VonElten, Alexander S. 1LT USA JFHO-NCR/MDW SJA; "Tooman, Joshua J CPT USARMY (US)"
Subject: Defense Motions
Date: Thursday, April 12, 2012 11:30:23 AM
Attachments: Def Response to Motion to Preclude.pdf
Def Response to Motion to Preclude.docx
Def Response to Motion to Preclude Redact.docx
Def Motion for Reconsideration - grand jury.pdf
Def Motion for Reconsideration - grand jury.docx
Def Motion for Reconsideration - grand jury Redact.docx
Security Expert Review.pdf

Ma'am,

The Defense has attached the following two motions:

- 1) Defense Response to Prosecution Motion to Preclude Reference to Actual Harm or Damage; and
- 2) Defense Request for Partial Reconsideration of Discovery Ruling

For each motion, the defense has attached a signed PDF version, a Word version, and a redacted Word version with yellow highlights. The yellow highlights were used to assist the Government in its review of the motions.

v/r

David

David E. Coombs, Esq.
Law Office of David E. Coombs
11 South Angell Street, #317
Providence, RI 02906

Toll Free: 1-800-588-4156

Local: (508) 689-4616

Fax: (508) 689-9282
coombs@armycourt martialdefense.com <<mailto:coombs@armycourt martialdefense.com>>

www.armycourt martialdefense.com <<http://www.armycourt martialdefense.com/>>

Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211)

Prosecution Response

to Defense Request for Partial
Reconsideration of Discovery Ruling

17 April 2012

RELIEF SOUGHT

The prosecution respectfully requests that the Court deny Defense Request for Partial Reconsideration of Discovery Ruling (hereinafter the "Defense Motion") because the rules of discovery do not support the defense's request for either the production of all grand jury proceedings in relation to the accused or WikiLeaks, or for *in camera* review of such materials under the standard set forth in Rule for Courts-Martial (RCM) 701(a)(2).

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the Defense bears the burden of persuasion and must prove any factual issues necessary to decide this motion by a preponderance of the evidence. See Manual for Courts-Martial, United States, Rule for Courts-Martial (R.C.M.) 905(c) (2008).

FACTS

The Army Criminal Investigation Command (CID), Federal Bureau of Investigation (FBI), and Diplomatic Security Service (DSS) are the only law enforcement authorities that participated in the joint investigation of the accused.

The FBI is a subordinate organization to the Department of Justice (DOJ). The FBI and DOJ are not Department of Defense (DOD) agencies operating under Title 10 status or subject to a military command.

The FBI files relating to the accused and WikiLeaks are classified. The DOJ files relating to the accused and WikiLeaks are, at a minimum, law enforcement sensitive and contain grand jury information. The prosecution has no authority to produce any FBI or DOJ files which have not already been produced to the defense.

On 23 March 2012, the Court ordered that the prosecution has a due diligence obligation to search, *inter alia*, the FBI files relevant to this case and to disclose to the defense that which is discoverable under RCM 701(a)(6) and Brady.¹ See Enclosure 1.

¹ For purposes of this Response, Brady includes its progeny.

APPELLATE EXHIBIT 49
PAGE REFERENCED:
PAGE OF PAGES

WITNESSES/EVIDENCE

The prosecution does not request any witnesses be produced for this motion. The prosecution requests that the Court consider the following enclosures to this motion in its ruling.

1. Ruling: Defense Motion to Compel Discovery, 23 March 2012 (Appellate Exhibit XXXVI).
2. Attachment F to Defense Motion to Compel Discovery, 16 February 2012 (Appellate Exhibit VIII).
3. Section V of Prosecution Supplement to Prosecution Proposed Case Calendar, 8 March 2012 (Appellate Exhibit XII).
4. Memorandum, *Task Force to Review Unauthorized Disclosure of Classified Information (FOUO)*, Secretary of Defense Robert Gates, 4 August 2010.

LEGAL AUTHORITY AND ARGUMENT

The prosecution requests that the Court deny the Defense Motion because the rules of discovery do not support the defense's request for either the production of all grand jury proceedings in relation to the accused or WikiLeaks or an *in camera* review of such materials under the standard set forth in RCM 701(a)(2).

I: RCM 701(a)(6) AND BRADY GOVERN DISCOVERY OF THE REQUESTED GRAND JURY MATERIALS.

On 23 March 2012, the Court ordered that the prosecution bears an obligation to search for, and disclose, information within the FBI file that is discoverable under RCM 701(a)(6) and Brady. See Enclosure 1, page 12 ("the Government will examine [the FBI files] for evidence that is favorable to the accused and material to either guilt or punishment").

RCM 701(a)(6) provides that the prosecution shall, as soon as practicable, disclose that which reasonably tends to negate guilt, reduce the degree of guilt, or reduce punishment. See RCM 701(a)(6). RCM 701(a)(6) implements the Supreme Court's decision in Brady. See Williams, 50 M.J. at 441; see also Brady v. Maryland, 373 U.S. 83, 87 (1963) (the prosecution shall disclose evidence favorable to the accused that is material to guilt or punishment). The prosecution bears an obligation to disclose to the defense any grand jury materials that are discoverable under these rules.

RCM 701(a)(2) provides that, upon defense request, the prosecution shall permit the defense to inspect materials "within the possession, custody, or control of military authorities" which are material to the preparation of the defense. See RCM 701(a)(2). The FBI is a subordinate organization to the DOJ, and neither organization is a DOD agency operating under Title 10 status or subject to a military command. Thus, the FBI and DOJ files are not within the possession, custody, or control of military authorities. RCM 701(a)(2) does not govern discovery of such files, to include any grand jury materials contained therein. Grand jury materials are only discoverable under RCM 701(a)(6) and Brady. This is consistent with the existing Order. See Enclosure 1.

The defense's request for the prosecution to produce the entire grand jury proceedings to the defense is not supported by any rule of discovery or production. See RCM 701(a)(6); see also Brady, 373 U.S. at 87; see also RCM 703(f) (relevant and necessary standard).

The defense's request for *in camera* review of such materials under the standard set forth in RCM 701(a)(2) is without legal merit. The prosecution continues its search of the FBI file for discoverable information under RCM 701(a)(6) and Brady, the applicable rules of discovery for material outside military authorities.

II: THE PROSECUTION SUPPLEMENTS ITS RESPONSE TO THE DEFENSE MOTION WITH THE FOLLOWING METHODOLOGY RELATING TO OTHER GOVERNMENT ORGANIZATIONS.

In light of the numerous government organizations involved and to cure any confusion or inconsistencies between the existing Court Order and the Defense Motion, the prosecution proffers which materials should be subject to discovery under RCM 701(a)(2), which files of government organizations the prosecution bears an obligation to search under Williams, and which files of organizations the prosecution has an ethical obligation to search.

A. The Discovery Standard under RCM 701(a)(2) Applies to Files within the Possession, Custody, or Control of Military Authorities For Which the Defense has Submitted a Specific Request.

Information within the possession, custody, or control of military authorities and specifically requested by the defense is discoverable, if material to the preparation of the defense. See RCM 701(a)(2). A specific request must provide "the prosecutor notice of exactly what the defense desires[.]" See United States v. Eshalomi, 23 MJ 12, 22 (CMA 1986) (citing United States v. Agurs, 427 U.S. 97, 106 (1976)). The prosecution proffers that DOD agencies operating under Title 10 status or subject to a military command are "military authorities" under RCM 701(a)(2). Thus, beyond the prosecution's own files and based on existing defense requests, only the *specifically-requested files* of the following government organizations are subject to review under RCM 701(a)(2) for discovery purposes:

(1) **Army Criminal Investigation Command (CID)**. The primary law enforcement organization within the Department of the Army focused on investigating the accused.

(2) **Defense Intelligence Agency (DIA)**. An intelligence agency within the DOD which operated the Information Review Task Force (IRTF), a DOD directed organization that "[f]ed a comprehensive [DOD] review of classified documents posted to the WikiLeaks website [...], and any other associated materials." See Enclosure 4.

The discovery standard under RCM 701(a)(2) does not apply to the files of other DOD agencies operating under Title 10 status or subject to a military command because the defense has not made a specific request for any such files.

B. The Court of Appeals for the Armed Forces in Williams Outlined the Scope of the Prosecution's Duty to Search for Discoverable Information.

The prosecution shall search the following files for discoverable information: (1) the files of law enforcement authorities that have participated in the investigation of the subject matter of the charged offenses; (2) investigative files in a related case maintained by an entity closely aligned with the prosecution; and (3) other files, as designated in a defense discovery request, that involved a specified type of information within a specified entity. See Williams, 50 M.J. at 441. The prosecution proffers that, based on the date of this response, it shall search the files of the following government organizations for discoverable information under each prong of Williams.

Law Enforcement Authorities

The only law enforcement authorities that participated in the joint investigation of the accused are as follows:

(1) **CID**. The primary law enforcement organization within the Department of the Army focused on investigating the accused.

(2) **FBI**. The primary law enforcement organization within the DOJ, focused on investigating matters related to the accused.

(3) **Diplomatic Security Service (DSS)**. The primary law enforcement organization within the Department of State (DOS), focused on investigating matters related to the DOS.

Closely Aligned Organizations

In addition to those above organizations, the prosecution proffers that only the following government organizations qualify as entities closely aligned with the prosecution:

(1) **DOS**. The accused is charged with compromising the DOS's documents and the prosecution intends to use additional information from the Department during its case-in-chief.

(2) **Government Agency**. The accused is charged with compromising this Government Agency's documents and the prosecution intends to use additional information from the Agency during its case-in-chief.

(3) **Office of the Director of National Intelligence (ODNI)**.² The prosecution intends to use information from this Department during its case-in-chief.

(4) **DOJ**. The prosecution collaborated with the federal prosecutors within the DOJ during the accused's investigation.³

² The prosecution is only referring to the ODNI proper, and not its subordinate organizations.

(5) **DIA.**⁴ The prosecution intends to use information from this Agency during its case-in-chief.

(6) **Defense Information Systems Agency (DISA).**⁵ The prosecution intends to use information from the Agency during its case-in-chief.

(7) **United States Central Command (CENTCOM).**⁶ The accused is charged with compromising the CENTCOM's documents and the prosecution intends to use additional information from the command during its case-in-chief.

(8) **United States Southern Command (SOUTHCOM).**⁷ The accused is charged with compromising the SOUTHCOM's documents and the prosecution intends to use additional information from the command during its case-in-chief.

Specific Requests

In addition to those above organizations and their related Williams category, the prosecution proffers that the defense submitted a request for a *specified type* of information only within the **Office of the National Counterintelligence Executive (ONCIX)**.⁸

C. In addition to the Search Requirements under Williams, the Prosecution has Sought Additional Information that it Believes to be Brady Material under its General Due Diligence Requirement.

In addition to the prosecution's discovery requirements under RCM 701(a)(2), RCM 701(a)(6), and Williams, the prosecution has an ethical obligation to search for potential Brady material that the prosecution has a good faith basis may exist in certain entities. See *U.S. Dep't of Army, Reg. 27-26, Rules of Professional Conduct for Lawyers* R. 1.1, R. 1.3, R. 3.8(d) (1 May

³ The prosecution is only referring to Main Justice and the District Prosecution Offices, and not its subordinate organizations.

⁴ This agency also falls within military authorities, pursuant to RCM 701(a)(2).

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

⁸ The prosecution and ONCIX are not closely aligned because they do not share a close working relationship. The prosecution's relationship with ONCIX is limited to the organization's review of certain classified information. The prosecution does not presently request reconsideration of the Court's Order dated 23 March 2012, where the Court identified ONCIX as being closely aligned with the prosecution, because the prosecution already bears an obligation to search the files of ONCIX based on a specific defense request.

1992) (AR 27-26). The prosecution has a good faith basis that the following government entities (not closely aligned with the prosecution) possess material that *could* be discoverable under RCM 701(a)(6) or Brady, and are not subject to a defense specific requests:

- (1) **Government Agency.**
- (2) **United States Cyber Command.**⁹
- (3) **More than Fifty Government Organizations with Limited Involvement.**

CONCLUSION

The prosecution respectfully requests that the Court deny the Defense Motion because the rules of discovery do not support the defense's request for either the production of all grand jury proceedings in relation to the accused or WikiLeaks or an *in camera* review under the standard set forth in RCM 701(a)(2).



ASHDEN FEIN
MAJ, JA
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 17 April 2012.



ASHDEN FEIN
MAJ, JA
Trial Counsel

⁹ This agency also falls within military authorities, pursuant to RCM 701(a)(2).

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC
U.S. Army, xxx-xx-
Headquarters and Headquarters Company,
U.S. Army Garrison, Joint Base Myer-
Henderson Hall, Fort Myer, VA 22211

)
) **RULING: DEFENSE MOTION**
) **TO COMPEL DISCOVERY**
)
)
)

) DATED: 23 March 2012
)

Defense moves the Court to compel discovery. Government opposes. After considering the pleadings, evidence presented, and argument of counsel, the Court finds and concludes the following:

Factual Findings:

1. In its Motion of 14 February 2012, the Defense moved the Court to compel the following discovery from the Government IAW RCM 701(a)(2) (Documents, tangible objects, and reports within the possession, custody, or control of military authorities that is material to the preparation of the defense), 701(a)(5)(Information to be offered by the Government at Sentencing), 701(a)(6)(Evidence favorable to the Defense) and 906(b)(7)(Motion for Appropriate Relief regarding discovery and production of evidence). The Government response is listed below each item:

a. FOIA Requests Regarding Video in Specification 2 of Charge II: A copy of any Freedom of Information Act (FOIA) request and any response or internal discussions of any such FOIA request that is related to the video that is the subject of Specification 2 of Charge II.

Government Response: On 3 October 2011, the Government produced all enclosures to any Freedom of Information Act (FOIA) response, specifically BATES 00000772-00000851. On 15 March 2012, the Government advised the Court it had given the Defense the information requested.

b. Quantico Video: The video of PFC Manning being ordered to surrender his clothing at the direction of CW4 James Averhart and his subsequent interrogation by CW4 Averhart on 18 January 2011. The Defense filed a preservation of evidence request over one year ago, on 19 January 2011 for this information. The Defense alleges the Government produced the video of PFC Manning being ordered to surrender his clothing, but not the video of the subsequent interrogation by CW4 Averhart. The Defense alerted the Government to the need to locate the additional video in a telephone conversation on 12 December 2011. The Defense proffered that the requested video is relevant to support the accused's claim of unlawful pretrial punishment. The Defense presented no evidence that the video exists.

Government Response: Upon Defense request, the United States promptly preserved all Quantico videos requested by Defense. On 6 December 2011, the United States produced all videos of the alleged Quantico incident, specifically BATES 00408902-00408903. The alleged video referenced by the Defense does not exist.

In an email to the Court dated 20 March 2012, the Defense accepted Trial Counsel's representation that the Government has provided the Defense with all videos provided to the Government by Quantico.

c. EnCase Forensic Images: An Encase forensic image of each computer from the Tactical Sensitive Compartmented Information Facility (T-SCIF) and the Tactical Operations Center (TOC) of Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division, Forward Operating Base (FOB) Hammer, Iraq. On 30 September 2010 CID requested preservation of hard drives used during the 2d BCT deployment to Iraq. The Defense submitted a preservation request for this evidence on 21 September 2011.

Government Response: On 21 September 2011 – more than one year after the accused's unit redeployed back to Fort Drum, New York – the Defense requested that the United States preserve these hard drives. The Government identified four commands or agencies that may possess hard drives responsive to this request and submitted a Request to Locate and Preserve Evidence to each command or agency. Those entities included: (1) 2d Brigade Combat Team, 10th Mountain Division (2/10 MTN); (2) the Federal Bureau of Investigation (FBI); (3) Third Army, United States Army Central (ARCENT); and (4) the Computer Crime Investigative Unit, U.S. Army Criminal Investigative Command (CCIU). The Government request to 2/10 MTN yielded the preservation of 181 hard drives, of which the United States has identified thirteen as being located within the SCIF during the unit's deployment to FOB Hammer. None of those thirteen hard drives contained the "bradley.manning" user profile. At the Article 39(a) session on 15 March 2012, the Government advised there were 14 hard drives responsive to the Defense discovery request. The Government argues the hard drives are not relevant and necessary for the Defense under RCM 703(f) and that, because they are classified, the rules of production under MRE 505 should govern whether the images are discoverable.

d. Damage Assessments and Closely Aligned Investigations: The following damage assessments and records from closely aligned investigations:

(1) Central Intelligence Agency: Any report completed by the WL Taskforce (WTF) and any report generated by the WTF under the direction of former Director Leon Panetta.

(2) Department of Defense: The damage assessment completed by the Information Review Task Force (IRTF) and any report generated by the IRTF under the guidance and direction of former Secretary of Defense Robert Gates. Additionally, the Defense requests all forensic results and investigative reports by any of the cooperating agencies in this investigation (DOS, FBI, DIA, the Office of the National Counterintelligence Executive (ONCIX), and the CIA).

(3) Department of Justice: Any documentation related to the DOJ investigation into the disclosures by WikiLeaks concerning PFC Bradley Manning, including any grand jury testimony or any information relating to any 18 U.S.C. § 2703(d) order or any search warrant by the government of Twitter, Facebook, Google or any other social media site.

(4) Department of State: The damage assessment completed by the DOS, any report generated by the task force assigned to review each released diplomatic cable, and any report or assessment by the DOS concerning the released diplomatic cables.

Government Response: The Government intends to disclose all relevant and necessary classified and unclassified grand jury testimony that the Government is authorized under the federal rules to the Defense. The Government: (1) confirms the existence of completed WTF and IRTF damage assessments; (2) confirms the existence of a damage assessment by DOS that is not complete; and (3) denies that ONCIX has produced an interim or final damage assessment. At the Article 39(a) session on 15 March 2012, the Government stated that it had no authority to disclose or discuss the requested damage assessments. The Government argues that Defense has not demonstrated that the damage assessments are relevant and necessary to an element of the offense or a legally cognizable defense and otherwise inadmissible in evidence under RCM 703(f) because the Defense is confusing prospective OCA classifications determinations assessing whether damage could occur (relevant to elements of charged offenses) with hindsight damage assessments determining what damage did occur (not relevant to elements of charged offenses). The Government further responded that it is unaware of any forensic results and investigative reports from within the DOS, FBI, DIA, ONCIX, or the CIA, that contributed to any law enforcement investigation.

2. The accused is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of disorders and neglects to the prejudice of good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting Government property, and two specifications of knowingly exceeding authorized access to a Government computer, in violation of Articles 92, 104, and 134, UCMJ, 10 U.S.C. §§ 892, 904, 934 (2010).

3. The Defense Motion to Compel the EnCase Forensic Images, the damage assessments from WTF, IRTF, and DOS, and forensic and investigative reports from DOS, FBI, DIA, ONCIX, or the CIA remain at issue.

4. The Defense submitted the following proffers of relevance and evidence in support of its Motion to Compel:

EnCase Forensic Images: The Defense requested an EnCase forensic image of each computer from the T-SCIF and the TOC of Headquarters and Headquarter Company, 2nd Brigade Combat Team, 10th Mountain Division, Forward Operating Base Hammer, Iraq.

a. **Proffer of relevance**: The Defense proffers that an EnCase Image would allow its forensic expert to inspect the 14 seized government computers from the T-SCIF and TOC. Such inspection would allow the Defense to discover whether it was common for Soldiers to add technically unauthorized computer programs to their computers and that the practice of the unit

was to tacitly authorize that addition of unauthorized programs including but not limited to: mIRC (a full featured Internet Relay Chat client for Windows that can be used to communicate, share, play or work with others on IRC networks); Wget (a web crawler program designed for robustness over slow or unstable network connections); GEOTRANS (an application program which allows a user to easily convert geographic coordinates among a wide variety of coordinate systems, map projections and datums); and Grid Extractor (a binary executable capable of extracting MGRS grids from multiple free text documents and importing them into a Microsoft Excel spreadsheet) to their computers. The Defense argues this information is relevant because the Government has charged PFC Manning with adding unauthorized software to his government computer in Specifications 2 and 3 of Charge III. The information is relevant to establish the defense theory that the addition of software not on the approved list of authorized software was authorized by the accused's chain of command through the practice of condoning and implicitly or explicitly approving the additions of such software.

b. **Evidence:** The Defense has provided the Court with a summary of what the defense asserts the following witnesses deployed with the accused testified to at the Article 32 investigation:

CPT Steven Lim – Soldiers listened to music and watched movies on their computers and saved music, movies, and games (unauthorized software).

CPT Casey Fulton – Soldiers saved music games, and computers to their computers. She added M-IRC Chat and Google Earth to her computer.

Mr. Jason Milliman – Soldiers added unauthorized games and music to their computers and was aware Soldiers were adding unauthorized software to their computers, although he did not believe the practice was common.

CPT Thomas Cherepko – He saw unauthorized music, movies, games, and unauthorized programs improperly stored on the T-Drive. He advised his immediate supervisor and the Brigade Executive Officer concerning the presence of unauthorized media on the T-Drive. Nothing was done.

Ms. Jihreah Showman – She and everyone else in the unit viewed M-IRC Chat as mission essential and everyone put it on their computers.

Damage Assessments and Closely Aligned Investigations: The Defense requested the following damage assessments and records from closely aligned investigations:

(1) **Central Intelligence Agency:** Any report completed by the WTF and any report generated by the WTF under the direction of former Director Leon Panetta.

(2) **Department of Defense:** The damage assessment completed by the Information Review Task Force (IRTF) and any report generated by the IRTF under the guidance and direction of former Secretary of State Robert Gates. Additionally, the Defense requests all forensic results and investigative reports by any of the cooperating agencies in this investigation (DOS, FBI, DIA, the Office of the national Counterintelligence Executive and the CIA).

(3) **Department of Justice:** The DOJ has conducted an investigation into the disclosures by WikiLeaks as referenced by Attorney General of the United States Eric H. Holder. The Defense requested any grand jury testimony and any information relating to any 18 U.S.C. §

2703(d) order or any search warrant by the government of Twitter, Facebook, Google or any other social media site that was relevant to PFC Bradley Manning.

(4) **Department of State:** The DOS formed a task force of over 120 individuals to review each released diplomatic cable. The task force conducted a damage assessment of the leaked cables and concluded that the information leaked either represented low-level opinions or was already commonly known due to previous public disclosures.

Proffer of Relevance for all Damage Reports: The Defense argues that evidence of damage assessments (whether favorable or not) are material to the preparation of the defense for the merits and sentencing IAW RCM 701(a)(2) and that, if the damage assessments are favorable, they are also relevant, helpful to the defense, and discoverable under RCM 701(a)(6) and *Brady v. Maryland*, 373 U.S. 83 (1963). Even if the extent of actual damage caused by the alleged leaks was not relevant to the merits, it is relevant discovery for the defense to prepare its presentencing case.

Evidence: The Defense provided its 30 November 2011 request to the Article 32 Investigation Officer (IO) for the production of evidence to include the damage assessments. That request includes the following:

a. 5 August 2010 creating the IRFT and 16 August 2010 letter from former Defense Secretary Robert Gates to Senator Carl Levin discussing the IRFT.

b. 8 November 2010 message from former CIA Director, Leon Panetta to CIA employees advising them that the Office of Security is directed to fully investigate the damage from WL. 22 December 2010 Washington Post article stating that the CIA established the WTF to assess the impact of exposure of thousands of leaked diplomatic cables.

c. 18 January 2011 Reuters article stating "Internal U.S. government reviews have determined that a mass leak of diplomatic cables caused only limited damage to U.S. interests abroad, despite the Obama administration's public statements to the contrary". The article listed the sources as two congressional aides familiar with briefings by State Department officials and Congress. The article further went on to state "National security officials familiar with the damage assessments being conducted by defense and intelligence agencies told Reuters the reviews so far have shown "pockets" of short-term damage, some of it potentially harmful. Long term damage to U.S. intelligence and defense operations, however, is unlikely to be serious, they said." And "But current and former intelligence officials note that while WL has released a handful of inconsequential CIA analytical reports, the website has made public few if any real intelligence secrets, including reports from undercover agents or ultra-sensitive technical intelligence reports, such as spy satellite pictures or communications intercepts."

All forensic results and investigative reports by any of the cooperating agencies in this investigation (DOS, FBI, DIA, the Office of the national Counterintelligence Executive and the CIA).

Proffer of relevance: None

Evidence: None

5. The Defense filed discovery requests for the EnCase Images, damage assessments, and forensic results and investigative reports by any of the cooperating agencies in the investigation. On 13 October 2011, the Defense made a specific request for *Brady* material, identifying the damage assessments. On 30 November 2011, the Government responded to the requests for the damage assessments under *Brady* that the Government has no knowledge of any *Brady* material in the possession of the CIA, Department of Defense, Department of Justice, or the Department of States, and it would furnish such records if it became aware of them and that the Government did not have authority to disclose the damage assessments. At or near 15 December 2011, the Government advised the Article 32 IO that the damage assessments were classified, that the Government does not have to discuss the substance of the damage reports, and that all but the IRTF are not under the control of military authorities. On 31 January 2012, the Government responded to Defense Discovery Requests for damage assessments stating it would not provide the damage requests because the defense failed to provide an adequate basis for its request and that the Defense was invited to renew its request with more specificity and an adequate basis for the request.

6. On 21 March 2015, the Court required the Government to respond to the following factual questions regarding each of the requested damage assessments. The Government response follows the question.

QUESTIONS:

1. Is each in the possession, custody, or control of military authorities?

Government Response: -

a. Defense Intelligence Agency (DIA) and the Information Review Task Force (IRTF)- Yes, the classified document itself is in the possession of military authorities (DIA); however, the document contains material from other Agencies and Departments outside the control of military authorities. The military controls the document itself, but not all the information within its four corners.

b. Wikileaks Task Force (WTF)- No.

c. Department of State (DOS) -DOS has not completed a damage assessment.

d. Office of the National Counterintelligence Executive (ONCIX)- ONCIX has not produced any interim or final damage assessments in this matter.

2. If no, what agency has custody of each of the damage assessments?

Government Response:

WTF - The Central Intelligence Agency has possession, custody, and control.

3. Does the Prosecution have access to the damage assessments?

Government Response:

a. DIA and IRTF- The prosecution was given limited access for the purpose of reviewing for any discoverable material. The prosecution only has control of the information within the document that is owned by the Department of Defense (military authority).

b. WTF - The prosecution was given very limited access for the purpose of reviewing for preparation of the previous motions hearing. The prosecution will have future access to complete a full review for *Brady* material, as outlined below.

4. Has the Prosecution examined each of the damage assessments for Brady material?

Government Response:

- a. DIA and IRTF- Yes.
- b. WTF -No.

4a. If yes, is there any favorable material?

Government Response:

DIA and IRTF- Yes; however, the United States has only found classified information that is "favorable to [the] accused that is material... to punishment." *Cone v. Bell*, 129 S.Ct. 1769, 1772 (2009); see also *Brady v. Maryland*, 373 U.S. 83, 87 (1973). The United States has not found any favorable material relevant to findings.

4b. If no, why not?

Government Response:

WTF- The prosecution has only conducted a cursory review of the damage assessment in order to understand what information exists within the Agency, and has not conducted a detailed review for *Brady* material. This process is ongoing and the prosecution will produce all "evidence favorable to [the]accused that is material to guilt or to punishment[]" if it exists, under the procedures outlined in MRE 505, *Cone v. Bell*, 129 S.Ct. at 1772; see also *Brady v. Maryland*, 373 U.S. at 87. Additionally, the United States is concurrently working with other Federal Organizations which we have a good faith basis to believe may possess damage assessments or impact statements, and will make such discoverable information available to the defense under MRE 505.

END OF QUESTIONS

7. No head of an executive or military department or government agency concerned has claimed a privilege to withhold classified information IAW MRE 505(c).

The Law:

1. Defense discovery in the military justice system is governed by the Constitutional standards set forth by the Supreme Court in *Brady v. Maryland*, 373 U.S. 83 (1963) and recently reaffirmed in *Smith v. Cain*, (slip opinion 10 January 2012), Article 46, UCMJ (Opportunity to Obtain Witnesses and Other Evidence), RCM 701 (Discovery), and, also, by RCM 703 (Production of Evidence) when the requested discovery is evidence not under the control of military authorities. For classified information, where the Government voluntarily agrees to disclose classified information in whole or in limited part to the accused, the provisions of MRE 505(g) apply. Where the Government seeks to use MRE 505 to withhold classified information, a privilege must be claimed IAW MRE 505(c). *U.S. v. Schmidt*, 60 M.J. 1 (C.A.A.F. 2004).

2. *Brady* requires the Government to disclose evidence that is favorable to the defense and material to guilt or punishment. Favorable evidence is exculpatory and impeachment evidence. *Brady* applies to classified information. The Government must either disclose evidence that is favorable to the defense and material to guilt or punishment, seek limited disclosure IAW MRE 505(g)(2), or invoke the privilege for classified information under MRE 505(c) and follow the procedures under MRE 505(f) and (i). The classified information privilege under MRE 505 does not negate the Government's duty to disclose information favorable to the defense and material to punishment under *Brady*. The Government may provide the information to the Court and move for limited disclosure IAW MRE 505(g)(2). If the privilege is claimed, MRE 505(i) allows the Government to propose alternatives to full disclosure.¹

3. Trial Counsel have a due diligence duty to review the files of others acting on the Government's behalf in the case for favorable evidence material to guilt or punishment. The scope of *Brady* due diligence is to examine files beyond the Trial Counsel's files is limited to:

(1) the files of law enforcement authorities that have participated in the investigation of the subject matter of the charged offense;

(2) investigative files in a related case maintained by an entity closely aligned with the prosecution; and

(3) other files, as designated in a defense discovery request, that involved a specified type of information within a specified entity.

For relevant files known to be under the control of another governmental entity, Trial Counsel must make that fact known to the Defense and engage in good faith efforts to obtain the material. *U.S. v. Williams*, 50 M.J. 436 (C.A.A.F. 1999).

4. Article 46, UCMJ (Opportunity to obtain witnesses and other evidence) provides in relevant part that trial counsel, defense counsel and the court-martial shall have equal opportunity to obtain witnesses and other evidence in accordance with such regulations as the President may prescribe.

5. The President promulgated RCM 701 to govern discovery and RCM 703 to govern evidence production. The rules work together when production of evidence not in the control of military authorities is relevant and necessary for discovery. *U.S. v. Graner*, 69 MJ 104 (C.A.A.F. 2010). The requirements for discovery and production of evidence are the same for classified and unclassified information under RCM 701 and 703 unless the Government moves for limited disclosure under MRE 505(g)(2) or claims the MRE 505 privilege for classified information. If the Government voluntarily discloses classified information to the defense, the protective order and limited disclosure provisions of MRE 505(g) apply. If, after referral, the Government invokes the classified information privilege, the procedures of MRE 505(f) and (i) apply.

¹ The parties have not presented the Court with any military cases directly on point. *Cone v. Bell*, 556 U.S. 449 (2009) does not address classified information disclosures required by the Government under *Brady*. Federal courts using the Classified Information Procedures Act (CIPA) recognize that *Brady* requires disclosure of evidence by the prosecution when it is both favorable to the accused and material either to guilt or punishment. See *U.S. v. Hanna*, 661 F.3d 271 (6th Cir. 2011).

6. Relevant discovery rules in RCM 701(Discovery) are:

a. RCM 701(a)(2) (Documents, tangible objects, reports) governs defense requested discovery of evidence material to the preparation of the defense that is within the possession, custody, or control of military authorities, whose existence is known or by due diligence should be known by the Trial Counsel. The rule provides for such discovery after service of charges upon the accused.

b. RCM 701(a)(6) (Evidence favorable to the defense) codifies *Brady* and provides that the trial counsel shall, as soon as practicable, disclose to the defense the existence of evidence known to the trial counsel which reasonably tends to: (A) negate the guilt of the accused to an offense charged; (B) reduce the degree of guilt of the accused of an offense charged; or (C) reduce the punishment.

c. RCM 701(f) provides that nothing in RCM 701 shall be construed to require the disclosure of information protected from disclosure by the Military Rules of Evidence. RCM 701(f) applies to discovery of classified information when the Government moves for limited disclosure under MRE 505(g)(2) of classified information subject to discovery IAW RCM 701 or when the Government claims a privilege under MRE 505(c) for classified information.

d. RCM 701(g) authorizes the military judge to regulate discovery. A military judge is not detailed to a court-martial until charges are referred for trial (Article 26(a) UCMJ).

7. RCM 703 (Production of Witnesses and Evidence) states in relevant part:

a. RCM 703(f)(1) provides that each party is entitled to the production of evidence which is relevant and necessary.

b. RCM 703(f)(4) provides that evidence under the control of the government may be obtained by notifying the custodian of the record of the time, place, and date the evidence is required and requesting the custodian to send or deliver the evidence. The custodian of the evidence may request relief on the grounds that the order of production is unreasonable or oppressive. After referral, the military judge may direct that the subpoena or order of production be withdrawn or modified. Subject to MRE 505 (Classified Evidence), the military judge may direct that the evidence be submitted for an *in camera* inspection in order to determine whether relief should be granted.

8. Both the discovery rules under RCM 701 and the evidence production rules under RCM 703 are grounded in relevance. In order to have the military judge compel release of evidence either as discovery under RCM 701 or as evidence production under RCM 703, the Defense must establish that the evidence is relevant either to the merits or to sentencing, *U.S. v. Graner*, 69 MJ 104 (C.A.A.F. 2010).

9. Prior to referral, the Government may decline to disclose information requested by the Defense IAW RCM 701 where the Government contests relevance and materiality. After referral, RCM 701(g) empowers the military judge to deny or regulate discovery to include

requiring the Government to produce the requested discovery for *in camera* review. RCM 701(g) does not require the Government to produce all discovery requested by the Defense to the Court for *in camera* review. As in this case, where the Government withholds discovery, the Defense may move for a Motion for Appropriate Relief to Compel Discovery IAW RCM 906(b)(7) and, where classified information is withheld by the Government, IAW MRE 505(d). Upon such a motion and a sufficient showing by the Defense of relevance and materiality, the Court may require the evidence to be produced for *in camera* review.

10. If classified discovery is at issue and the government agrees to disclose classified information to the defense, the military judge shall enter an appropriate protective order if the government requests one IAW MRE 505(g)(1) or allow the Government to move for limited disclosure under MRE 505(g)(2).

11. If classified discovery detrimental to national security is at issue and the government does not wish to disclose the classified information in part or in whole to the defense, the government must claim a privilege under MRE 505(c). There is no privilege under MRE 505 for classified information unless the privilege is claimed by the head of the executive or military department or government agency concerned based on a finding that the information is properly classified and that disclosure would be detrimental to the national security.

12. MRE 505(e) (Pretrial Session) states in relevant part that after referral and prior to arraignment any party may move for a session under Article 39(a) to consider matters relating to classified information in connection with the trial. Following such a motion or *sua sponte* the military judge promptly shall hold a session to establish the timing of requests for discovery, the provision of notice under MRE 505(h), and the initiation of procedures under MRE 505(i). In addition the military judge may consider any matters that relate to classified information or that may promote a fair and expeditious trial.

Analysis:

1. No government entity in possession of any discovery at issue has claimed a privilege under MRE 505(c). Thus, *Brady*, RCM 701(a)(2), 701(a)(6), and 701(g) govern discovery of both classified and unclassified information. MRE 505(g) also applies when the Government voluntarily discloses classified information. RCM 703(f) requires that discovery of evidence outside the control of military authorities be relevant and necessary.

2. The 14 hard drives for which the EnCase Images are requested are within the possession, custody, or control of military authorities. Some of the information in the IRFT damage assessment is under the possession, custody, or control of military authorities. The DOS and WTF damage assessments are in the possession, custody, and control of the Department of State and the Central Intelligence Agency, respectively.

3. Because no privilege has been invoked under MRE 505(c) and the Government has not moved for limited disclosure IAW RCM 505(g)(2), RCM 701(f) does not preclude disclosure of classified information that is material to the preparation of the defense under RCM 701(a)(2) or classified information that is favorable to the defense under RCM 701(a)(6).

4. Under Brady and RCM 701(a)(6), the Government has a due diligence duty to search for evidence that is favorable to the defense and material to guilt or punishment. This includes a due diligence to search any damage assessment pertaining to the alleged leaks in this case made by the CIA, DoD, DOJ, and DOS. These agencies are entities closely aligned with the prosecution in this case. The Government must disclose any favorable classified information from the damage assessments that is material to punishment, move for limited disclosure under MRE 505(g)(2), or claim the privilege IAW MRE 505(c).

5. The Government has examined the IRTF damage assessment and has found information favorable to the accused that is material to punishment. The Court further finds that the IRTF damage assessment is relevant and necessary for discovery under *Brady* and RCM 701(a)(6).

6. The Court finds that the WTF and DOS damage assessments may contain evidence favorable to the accused that is material to punishment. The Court finds that these damage assessments are relevant and necessary for the Government to examine for *Brady* material.

7. The Court finds all 3 damage assessments relevant and necessary for the Court to conduct an *in camera* review to determine whether they contain information that is favorable to the accused and material to punishment under *Brady*, whether they contain information relevant and favorable to the accused under RCM 701(a)(6), and whether they contain information material to the preparation of the defense under RCM 701(a)(2).

8. The Government has advised the Court it is "unaware" of any forensic results or investigative files relevant to this case maintained by DOS, FBI, DIA, ONCIX, and CIA. These agencies are closely aligned to the Government in this case. The Government has a due diligence duty to determine whether such forensic results or investigative files that are germane to this case are maintained by these agencies. The Government will advise the Court whether they have contacted DOS, FBI, DIA, ONCIX, and CIA and that each of these agencies have stated to the government that no such forensic results or investigative files exist.

9. The Court finds that a complete search of the relevant 14 hard-drives of computers from the Tactical Sensitive Compartmented Information Facility (T-SCIF) and the Tactical Operations Center (TOC) of Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division, Forward Operating Base (FOB) Hammer, Iraq is not material to the preparation of the defense for specifications 2 and 3 of Charge III IAW RCM 701(a)(2). At least some of the information on the hard drives is classified. The witnesses at the Article 32 investigation testified that Soldiers would save unauthorized music, movies, games, and other programs such as Google Earth and M-IRC Chat. The Defense has evidence from the Article 32 witnesses to further the defense theory. Although a complete search is not material, the Court will direct the Government to search each of the 14 hard drives Wget, M-IRC Chat, Google Earth, movies, games, music, and any other specifically requested program from the Defense. The Government will disclose the results of the search to the Defense under MRE 701(g)(1) and 505(g)(2). The Defense may renew its Motion to Compel Encase Forensic Images after receipt of the results of the Government search.

RULING: The Defense Motion to Compel Discovery is **Granted in Part**.

ORDER:

1. The Government will **immediately** begin the process of producing the damage assessments that are outside the possession, custody, or control of military authorities IAW RCM 703(f)(4)(A). If necessary, the Government shall prepare an order for the Court to sign for each custodian.
2. The Government will **immediately** cause an inspection of the 14 hard drives as provided in paragraph (Analysis 9) above. On or before **30 March 2012**, Defense will provide a list of additional terms the Government wants the Government to add to its search of the 14 hard drives. On or before **20 April 2012**, the Government will provide the results of the search.
3. The Government shall contact DOS, FBI, DIA, ONCIX, and CIA to determine whether these agencies contain any forensic results or investigative files relevant to this case. The Government will notify the court NLT **20 April 2012** whether any such files exist. If they do exist, the Government will examine them for evidence that is favorable to the accused and material to either guilt or punishment.
4. By **20 April 2012** the Government will notify the Court with a status of whether it anticipates any government entity that is the custodian of classified evidence that is the subject of the Defense Motion to Compel will seek limited disclosure IAW MRE 505(g)(2) or claim a privilege IAW MRE 505(c) for the classification under that agency's control.
5. By **18 May 2012** the Government will disclose any unclassified information from the 3 damage assessments that is favorable to the accused and material to guilt or punishment and provide any additional unclassified information from the damage assessments to the Court for in camera review IAW RCM 701(g)(2).
6. By **18 May 2012** the Government will identify what classified information from the 3 damage reports it found that was favorable to the accused and material to guilt or punishment. By **18 May 2012** the Government will disclose all classified information from the 3 damage assessments to the Court for *in camera review* IAW RCM 701(g)(2) or, at the request of the Government, *in camera review* for limited disclosure under MRE 505(g)(2). By **18 May 2012**, if the relevant Government agency claims a privilege under MRE 505(c) and the Government seeks an *in camera* proceeding under MRE 505(i), the Government will move for an *in camera* proceeding IAW MRE 505(i)(2) and (3) and provide notice to the Defense under MRE 505(i)(4)(A).

So **ORDERED:** this 23rd day of March 2012.



DENISE R. LIND

COL, JA

Chief Judge, 1st Judicial Circuit

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army, xxx-xx-)

Headquarters and Headquarters Company, U.S.)

Army Garrison, Joint Base Myer-Henderson Hall,)
Fort Myer, VA 22211)

**DEFENSE DISCOVERY
REQUEST**

DATED: 13 May 2011

1. In accordance with the Rules for Courts-Martial and the Military Rules of Evidence, Manual for Courts-Martial, United States, 2008, Article 46, Uniform Code of Military Justice, and other applicable law, request for supplemental discovery is hereby made for the charged offenses in the case of United States v. Bradley F. Manning.

2. The defense requests that the government continue with its obligation to provide discovery in response to each item listed in its previous discovery requests on 29 October 2010, 15 November 2010, 8 December 2010, 10 January 2011, and 16 February 2011 and to also respond to the below requested discovery.

3. The defense requests that the government produce any and all documents (sworn or signed statements, photographs, emails etc.), tangible items (books, papers, etc.), and reports (investigative summaries, damage assessments, Original Classification Authority (OCA) determinations, etc.), conducted by the United States Army, the Department of Defense, the Department of Justice, the National Security Agency, the Defense Intelligence Agency, the Department of Homeland Security Office of Intelligence and Analysis, the Central Intelligence Agency, the Federal Bureau of Investigation, and the Bureau of Diplomatic Security (DS). The trial counsel, upon defense request, has an affirmative obligation to seek out requested evidence that is in the possession of the government even if that evidence is not already in the immediate possession of the trial counsel. *United States v. Williams*, 50 M.J. 436, 441 (C.A.A.F. 1999); *United States v. Bryan*, 868 F.2d 1032, 1036 (9th Cir. 1989); *United States v. Brooks*, 966 F.2d 1500, 1503 (1992) (the government is considered to have possession of information that is in the control of agencies that are "closely aligned with the prosecution").


4. The defense requests any *Brady* material in the government's possession. *Brady v. Maryland*, 373 U.S. 83 (1963) (holding that due process requires the government to turn over exculpatory evidence in its possession). The defense also requests any *Jencks* material in the government's possession. *Jencks v. United States*, 353 U.S. 657 (1957) (holding that, in a criminal prosecution, the government may not withhold documents relied upon by government witnesses, even where disclosure of those documents might damage national security matters). Specifically, the defense requests copies of all statements, oral or written, by any witnesses. The defense also requests any evidence in

the government's possession that contradicts or is inconsistent with the government's theory of the case.

5. The defense requests that the government inform the defense counsel if it does not intend to comply with any specific provision of this request.

6. It is understood that this is a continuing request.

7. A copy of this request was served on Trial Counsel by e-mail on 13 May 2011.



DAVID EDWARD COOMBS
Civilian Defense Counsel

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, xxx-xx- [REDACTED]

Headquarters and Headquarters Company, U.S.
Army Garrison, Joint Base Myer-Henderson Hall,
Fort Myer, VA 22211

DEFENSE REQUEST TO
PRESERVE EVIDENCE

DATED: 21 September 2011

1. In accordance with the Rules for Courts-Martial (R.C.M.) 701(a) and (c), Manual for Courts-Martial, United States, 2008, Article 46, Uniform Code of Military Justice, and other applicable law, defense counsel in the above entitled case respectfully request that the U.S. Government preserve all computer forensic evidence obtained in this case.

2. The Defense specifically requests that the Government preserve all the hard drives from the Tactical Sensitive Compartmented Information Facility (T-SCIF) and the Tactical Operations Center (TOC) of Headquarters and Headquarter Company (HHC), 2nd Brigade Combat Team (BC1), 10th Mountain Division, Forward Operating Base (FOB) Hammer, Iraq and provide an EnCase forensic image of each computer to the defense for its inspection. The defense also requests an EnCase forensic image of any other computer seized by the Government in this case.

3. In accordance with R.C.M. 701(c), "[e]ach party shall have equal opportunity to ... inspect evidence." Defense counsel is requesting an equal opportunity to inspect the hard drives from the T-SCIF and TOC of HHC, 2nd BC1, 10th Mountain Division, FOB Hammer, Iraq. The defense believes the requested evidence constitutes *Brady* material under *Brady v. Maryland*, 373 U.S. 83 (1963).

4. A copy of this request was served on Trial Counsel by e-mail on 21 September 2011.


DAVID EDWARD COOMBS
Civilian Defense Counsel

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army. xxx-xx- [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

**DEFENSE DISCOVERY
REQUEST**

DATED: 13 October 2011

1. In accordance with the Rules for Courts-Martial and the Military Rules of Evidence, Manual for Courts-Martial, United States, 2008, Article 46, Uniform Code of Military Justice, and other applicable law, request for discovery is hereby made for the charged offenses in the case of United States v. Bradley E. Manning.

a. A copy of any adverse administrative or UCMJ action, all supporting documentation, and any rebuttal materials to such action based upon the 15-6 investigation conducted by LTJG Robert L. Caslen Jr. or any other governmental investigation, with regards to any individual that was the subject of such an adverse action in relation to the alleged leak of classified information in this case. The request includes, but is not limited to, the following individuals: COL. David M. Miller, COL Paul R. Walter, LTC Brian D. Kerns, LTC Rodney Garfield, LTC Randolph Wardle, MAJ Eric Davis, MAJ Eric Graham, MAJ Jason A. Morrow, MAJ Clifford D. Clausen, MAJ Elijah A. Dreher, CPT Matthew W. Freeburg, 1SG Eric H. Usbeck, CPT Thomas M. Cherepko, CPT Steven J. Lim, CPT Barclay D. Keay, CPT Casey Martin, 1LT Tanya M. Gaag, 1LT Elizabeth A. Fields, CW2 Joshua D. Ehresman, CW2 Chad Eastep, CW2 Alfred Lyons, WO1 Kyle J. Balonek, SFC Paul D. Adkins, SSG Lawrence W. Mitchell, SPC Daniel W. Padgett, and PFC Jirleah W. Showman.

b. An inspection of all seized governmental computers from the Tactical Sensitive Compartmented Information Facility (T-SCIF) and Tactical Operations Center (TOC) of Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BC1), 10 Mountain Division, Forward Operating Base (FOB) Hammer, Iraq for the presence of any and all unauthorized computer programs to include, but not limited to: mIRC (a full featured Internet Relay Chat client for Windows that can be used to communicate, share, play or work with others on IRC networks); Wget (a web crawler program designed for robustness over slow or unstable network connections); GEOTRANS (an application program which allows a user to easily convert geographic coordinates among a wide variety of coordinate systems, map projections and datums); and Grid Extractor (a binary executable capable of extracting MGRS grids from multiple free text documents and importing them into a Microsoft Excel spreadsheet).

c. The defense requests any *Brady* material in the government's possession. *Brady v. Maryland*, 373 U.S. 83 (1963) (holding that due process requires the government to turn over exculpatory evidence in its possession). The defense also requests any *Jencks* material in the government's

possession. *Jencks v. United States*, 353 U.S. 657 (1957) (holding that, in a criminal prosecution, the government may not withhold documents relied upon by government witnesses, even where disclosure of those documents might damage national security matters). The defense specifically requests the following information:

i) White House: any report or recommendation concerning the alleged leaks in this case by Mr. Russell Travers, National Security Staff's Senior Advisor for Information Access and Security Policy. Mr. Travers was tasked to lead a comprehensive effort to review the alleged leaks in this case. Any and all documentation related to President Barack H. Obama's order for an investigation and a government wide-review of how agencies safeguard sensitive information. Additionally, any and all documents related to the steps the administration is considering regarding these leaks and the nature of the criminal investigation underway into how the documents were made public as referenced by former White House Press Secretary Robert Gibbs. Any assessment given, or discussions concerning, the Wikileaks disclosures by any member of the government to President Obama. Any e-mail, report, assessment, directive, or discussion by President Obama to the Department of Defense, Department of State or Department of Justice;

ii) President's Intelligence Advisory Board: any report or recommendation concerning the alleged leaks in this case by Chairman Chuck Hagel or any other member of the Intelligence Advisory Board;

iii) Central Intelligence Agency: any report, damage assessment or recommendation by the Wikileaks Task Force or any other CIA member concerning the alleged leaks in this case. Any internal or external memorandums addressing the investigation of Wikileaks, PFC Bradley Manning or the nature of the Office of Security's investigation into these matters;

iv) Department of Defense: All forensic results and investigative reports by the Department of Defense regarding the information obtained by Wikileaks and the results of any joint investigation with the Federal Bureau of Investigation (FBI) as referenced by Former Secretary of Defense Robert M. Gates. Additionally, any specific damage assessment by the Department of Defense regarding the disclosure of classified documents and videos, the subject of this case, by WikiLeaks. Specifically, any report by the Information Review Task Force (IRTF) that was responsible for leading a comprehensive Department of Defense review of classified documents obtained by the Wikileaks website and any other associated materials;

v) Department of Justice: Any and all documentation related to the Department of Justice investigation into the alleged leaks by WikiLeaks as referenced by Attorney General of the United States Eric H. Holder;

vi) Department of State: Any and all documentation relating to a review of the alleged leaks in this case and any specific damage assessment by the Department of State regarding the disclosure of diplomatic cables, the subject of this case, by Wikileaks;

vii) Office of the Director of National Intelligence (ODNI): Any and all documentation relating to any review or damage assessment conducted by ODNI or in cooperation with any other government agency;

viii) Other Government Intelligence Agencies: Any and all documents relating to any task force or other governmental intelligence agency review of the various alleged leaks in this case to include, but not limited to, any damage assessment based upon the alleged leaks or any corrective action taken by the United States Government due to the alleged leaks; AND

ix) House of Representatives: Results of any inquiry and testimony taken by House of Representative oversight committee led by Representative Darrell Issa. The committee discussed the actions of Wikileaks, the actions of Attorney General Eric Holder, and the investigation of PFC Bradley Manning.

d. The defense requests a copy of the Preliminary Inquiry Report. According to Department of Defense (DoD) 5105.21-M-1, once an SCI Security Official determines that a security violation has occurred, the SCI Security Official must report the violation within 72 hours of discovery to the appropriate Senior Officials of the Intelligence Community (SOIC) or Senior Intelligence Officer (SIO).

e. The defense requests a copy of the Damage Assessment of Compromised Information that is required to be submitted to the Special Security Officer (SSO) under DoD 5105.21-M-1 once an SCI Security Official determines that a security violation has occurred. The damage assessment is supposed to contain the date of the assessment; the name and office symbol conducting the assessment; subject/title, date, number, originator and original classification of document; whether the document can be declassified or downgraded, either in whole or in part; justification for classification (the specific statements in the document which are classified, the basis for classification, and a complete bibliography of all classified source materials used in preparation of the document); whether the classified information identified is accurate; whether the classified information identified was the subject of any official release; and whether the information identified as classified can be edited for the purpose of prosecution.

f. The defense requests a copy of the final security violation investigation report submitted to the SSO DoD/ Defense Intelligence Agency (DIA) under DoD 5105.21-M-1. The report is used to assess intent, location of the incident, risk of compromise, sensitivity of information, and mitigating factors in arriving at a final analysis of the incident.

g. A copy of all SCI security management and self-inspection reports for the T-SCIF of HHC, 2nd BCT, 10 Mountain Division, FOB Hammer, Iraq.

2. The defense requests that the government informs the defense counsel if it does not intend to comply with any specific provision of this request.

3. It is understood that this is a continuing request.

4. A copy of this request was served on Trial Counsel by email on 13 October 2011.



DAVID EDWARD COOMBS
Civilian Defense Counsel

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, xxx-xx-██████

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,
Fort Myer, VA 22211

**DEFENSE DISCOVERY
REQUEST**

DATED: 15 November 2011

1. In accordance with the Rules for Courts-Martial and the Military Rules of Evidence, Manual for Courts-Martial, United States, 2008, Article 46, Uniform Code of Military Justice, and other applicable law, request for discovery is hereby made for the charged offenses in the case of United States v. Bradley E. Manning.

2. The Defense requests that the Government respond to each item listed in its previous discovery requests and to also respond to the following additional discovery:

- a) Whether any NIPR or SIPR computer within the 2d BCT T-SCIF or Supply Annex required an end-user to have their ID CAC Card in the computer;
- b) The required log-in procedure for use of the HP laptop, touch smart TS2, serial number CNF8492K3S;
- c) All NIPR and SIPR logs for any computer within the 2d BCT T-SCIF from 1 November 2009 to 27 May 2010;
- d) An EnCase forensic image of any computer seized by the government and all other information relied upon by the government to claim information leaked to Wikileaks was obtained by any terrorist group such as Al-Qaeda or Hizb-L Islami Gulbuddin (HIG);
- e) A current curriculum vitae for each forensic expert who has worked on this case for the government;
- f) Any classification review and damage assessment for documents related to Specification 8 and 9 of Charge II;
- g) Any classification review and damage assessment for the document related to Specification 15 of Charge II.

3. The Defense requests that the Government provide notice in writing if it does not intend to comply with any specific provision of this request.

4. It is understood that this is a continuing request.

5. A copy of this request was served on Trial Counsel by email on 15 November 2011.

A handwritten signature in black ink, appearing to read 'D. Coombs', with a stylized, sweeping flourish at the end.

DAVID EDWARD COOMBS
Civilian Defense Counsel

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, xxx-xx-[REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

)
)
) **DEFENSE DISCOVERY**
) **REQUEST**
)
)
)

) DATED: 16 November 2011
)

1. In accordance with the Rules for Courts-Martial and the Military Rules of Evidence, Manual for Courts-Martial, United States, 2008, Article 46, Uniform Code of Military Justice, and other applicable law, request for discovery is hereby made for the charged offenses in the case of United States v. Bradley E. Manning.

2. The Defense requests that the Government respond to each item listed in its previous discovery requests and to also respond to the following additional discovery:

a) An EnCase forensic image of any computer seized by the government and all other information relied upon by the government to claim information alleged to have been disclosed in this case was in the possession of an unauthorized individual in December of 2009 (according to the Government, this individual was a representative of WikiLeaks);

b) Any damage assessment or review completed in this case either by or with the assistance of the Defense Intelligence Agency, the Office of the National Counterintelligence Executive or any other governmental agency;

3. The Defense requests that the Government provide notice in writing if it does not intend to comply with any specific provision of this request.

4. It is understood that this is a continuing request.

5. A copy of this request was served on Trial Counsel by email on 16 November 2011.

/s/
DAVID EDWARD COOMBS
Civilian Defense Counsel

Preservation Request, dated 14 June 2011). After reviewing tens-of-thousands of pages of documents from multiple federal organizations pursuant to these requests, trial counsel are confident that other analytic products produced within the intelligence community contain references to information otherwise "owned" by other organizations within the intelligence community; therefore, any production of this material will likely take time to coordinate because of all the parties involved.

V: ORIGINAL CLASSIFICATION AUTHORITIES

1. As discussed above, the case involves multiple federal organizations because of the scale of the alleged disclosures of classified information. These organizations fall within the three categories below. If a federal organization contains an "*" next to its name, the United States anticipates that documents originating from that federal organization will contain information from multiple OCAs.

A. Federal organizations with equities in charged documents or digital forensic evidence.

- (1) Department of State*
- (2) Office of the Director of National Intelligence
- (3) Defense Information Systems Agency
- (4) United States Central Command
- (5) United States Southern Command
- (6) Government Agency*
- (7) United States Cyber Command

B. Other federal organizations with equities, but not in charged document or digital forensic evidence.

- (1) Federal Bureau of Investigation
- (2) Government Agency*
- (3) Department of Defense*
- (4) Defense Intelligence Agency*

C. Other federal organizations that have very limited involvement

2. The United States estimates that any Court order to disclose classified information, will likely require coordination with multiple federal organizations in categories (1) and (2), and roughly estimates forty-five to sixty days to aggressively coordinate a response across all equity holders. Within the sixty day window, it would likely take approximately one to two weeks to identify equity holders and distribute the product amongst the relevant federal organizations and their OCAs. Thirty days to analyze the product to identify the sources of classified information and evaluate the level of protection that must be given to that information. Two additional weeks for the OCAs to coordinate a response, for example to approve full disclosure, limited disclosure, some variation, or invoke the privilege. If an OCA invokes the classified information privilege, it may take additional time to conduct a classification review and route the document to the

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Prosecution Response

to Defense Request for Partial
Reconsideration of Discovery Ruling

Enclosure 4

17 April 2012

APPELLATE EXHIBIT 49
PAGE REFERENCED: _____
PAGE ____ OF ____ PAGES

UNCLASSIFIED//FOR OFFICIAL USE ONLY



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

AUG 5 2010

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM
EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

Subject: Task Force to Review Unauthorized Disclosure of Classified Information (FOUO)

(U//FOUO) On July 28, 2010, I directed the Director, Defense Intelligence Agency (DIA) to establish an Information Review Task Force (IRTF) to lead a comprehensive Department of Defense (DoD) review of classified documents posted to the WikiLeaks website (www.wikileaks.org) on July 25, 2010, and any other associated materials. Department of Defense Components should provide DIA any assistance required to ensure the timely completion of the review.

(U//FOUO) The IRTF will review the impact of the unauthorized disclosure of classified information specified above. The IRTF will coordinate throughout the Intelligence Community in conducting this time-sensitive review and integrate its efforts with those of the National Counterintelligence Executive.

(U//FOUO) The IRTF will provide regular updates to the Office of the Secretary of Defense (OSD) on its findings. A more comprehensive interim report will be provided as the effort progresses. That report will include the following items:

- (U//FOUO) Any released information with immediate force protection implications;
- (U//FOUO) Any released information concerning allies or coalition partners that may negatively impact foreign policy;
- (U//FOUO) Any military plans;

OSD 09134-10



UNCLASSIFIED//FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

0028 10 CID221 10117

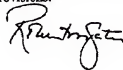
UNCLASSIFIED//FOR OFFICIAL USE ONLY

- (U//FOUO) Any intelligence reporting;
- (U//FOUO) Any released information concerning intelligence sources or methods;
- (U//FOUO) Any information on civilian casualties not previously released;
- (U//FOUO) Any derogatory comments regarding Afghan culture or Islam; and
- (U//FOUO) Any related data that may have also have been released to WikiLeaks, but not posted.

A final report will be produced once all documents are assessed.

(U//FOUO) The RTF is the single DoD organization with authority and responsibility to conduct the DoD review regarding this unauthorized disclosure. By separate tasking, I am directing USD(I) to conduct an assessment of the Department's procedures for accessing and transporting classified information.

(U//FOUO) This review is separate from, and unrelated to, any criminal investigation of the leaked information. The assessment and review of the leaked documents is not intended to, and shall not limit in any way, the ability of Department, Federal Bureau of Investigation or any other federal criminal investigators, trial counsel and prosecutors to conduct investigative and trial proceedings in support of possible prosecutions under the Uniform Code of Military Justice or federal criminal provisions.



cc:
Director of National Intelligence
Director, Central Intelligence Agency
Assistant Secretary of State for Intelligence & Research
National Counterintelligence Center

UNCLASSIFIED//FOR OFFICIAL USE ONLY

LAW ENFORCEMENT SENSITIVE

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC
U.S. Army, xxx-xx-
Headquarters and Headquarters Company, U.S.
Army Garrison, Joint Base Myer-Henderson Hall,
Fort Myer, VA 22211

**DEFENSE REPLY TO
PROSECUTION RESPONSE
TO DEFENSE REQUEST FOR
PARTIAL RECONSIDERATION
OF DISCOVERY RULING**

18 April 2012

RELIEF SOUGHT

1. In accordance with the Rules for Courts-Martial (R.C.M.) 701(a)(2), 701(a)(6), and 905(f), Manual for Courts-Martial (M.C.M.), United States, 2008; Article 46, Uniform Code of Military Justice (UCMJ); and the Fifth and Sixth Amendments to the United States Constitution, the Defense respectfully requests that the Court reconsider, in part, its ruling on the compelled discovery. Specifically, the Defense requests that this Court find that the grand jury materials are in the possession, custody and control of military authorities within the meaning of R.C.M. 701(a)(2) and order them to be produced to the Defense, or for *in camera* review.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. As the moving party, the Defense has the burden of persuasion. R.C.M. 905(c)(2), 905(f). The burden of proof is by a preponderance of the evidence. R.C.M. 905(c)(1), 905(f).

FACTS

3. In the absence of knowledge to the contrary, the Defense adopts as true the Government's statements about the involvement of various agencies in this case. Thus, there are at least three type of entities involved in this case that are relevant for the purpose of this motion:

- a) Military organizations/entities;
- b) Entities that participated in a joint investigation;
- c) Other "closely aligned" agencies.

Based on the Prosecution's Response to Defense Request for Partial Reconsideration of Discovery Ruling [hereinafter "Government Response"], the Defense has organized these agencies accordingly:

a) Military Organizations/Entities

Army Criminal Investigation Command (CID). The primary law enforcement organization within the Department of the Army focused on investigating the accused.

Defense Intelligence Agency (DIA). An intelligence agency within the DOD which operated the Information Review Task Force (IRTF), a DOD directed organization that “[led] a comprehensive [DOD] review of classified documents posted to the WikiLeaks website [...], and any other associated materials.”

Defense Information Systems Agency (DISA)

United States Central Command (CENTCOM) and United States Southern Command (SOUTHCOM)

b) Joint Investigations

FBI. The primary law enforcement organization within the DOJ, focused on investigating matters related to the accused.

Diplomatic Security Service (DSS). The primary law enforcement organization within the Department of State (DOS), focused on investigating matters related to the DOS.

c) Closely Aligned Organizations

Department of State. The accused is charged with compromising the DOS’s documents and the Government intends to use additional information from the Department during its case-in-chief.

DOJ. The Government collaborated with the federal prosecutors within the DOJ during the accused’s investigation.

Government Agency. The accused is charged with compromising this Government Agency’s documents and the Government intends to use additional information from the Agency during its case-in-chief.

Office of the Director of National Intelligence (ODNI). The Government intends to use information from this Department during its case-in-chief.

ONCIX. The Government disputes that ONCIX is closely aligned. Government Response, p. 5, fn 8. The Court found in its ruling that ONCIX is a closely aligned agency. See Ruling: Defense Motion to Compel Discovery, p. 11, paras. 4, 8.

4. The Government is resisting producing the grand jury testimony under R.C.M. 701(a)(2) on the following basis:

the FBI is a subordinate organization to the DOJ, and neither organization is a DOD agency operating under Title 10 status or subject to a military command. Thus, the FBI and DOJ files are not within the possession, custody, or control of military authorities. RCM 701(a)(2) does not govern discovery of such files, to include any grand jury materials contained therein. Grand jury materials are only discoverable under RCM 701(a)(6) and *Brady*.

Government Response, p. 2.¹

5. Over a month ago, the Defense predicted this latest tactic by the Government to deny discovery:

The Government has not once in the past year and a half objected to any of the Defense's discovery requests on the basis that the information sought is not in the "possession, custody, or control of military authorities." Rather, the Government has simply said that the requests were not specific enough or that it did not believe the material was relevant or necessary under R.C.M. 703. In the event that the Government now switches its "game plan" to deny discovery, it should be estopped from arguing that any of the Defense's requested information is not in the "possession, custody, or control of military authorities."

Reply to the Defense Motion to Compel Discovery, p. 8, fn. 8. Not surprisingly, now that the Government's previous attempts to deny discovery to the Defense have failed, the Government is raising for the first time the argument that the requested files are not within the possession, custody or control of military authorities. The Defense would ask that the Court view with skepticism the *bona fides* of the Government's latest attempt to deny discovery to the Defense. In short, the Government has resisted producing this evidence on various bases: that the request was not specific enough, that there was no adequate basis for the request, that much of the material was classified, etc. See Government Response to Defense Motion to Compel Discovery, p. 14. Now that the Government has lost all those battles, it seeks to erect a new obstacle for the Defense: that even though the FBI participated in a joint investigation of the accused and even though the Government has ready access to this material, such material is not in the possession, custody and control of military authorities.

¹ The Defense would point out that the Government's statement is plainly wrong on its face. Even if the materials were not discoverable under R.C.M. 701(a)(2)—which the Defense submits that they are—the materials would be discoverable under R.C.M. 703, and not only under R.C.M. 701(a)(6)/*Brady*. Since the issue here does not turn on the scope of the Government's *Brady* search, but rather on whether the grand jury materials are in the possession, custody and control of military authorities for purposes of R.C.M. 701(a)(2), the Defense will not respond specifically to the Government's outline of what it believes its *Brady* responsibilities to be. The Defense reserves the right, if necessary, to challenge the Government's submissions in this respect at a later time.

ARGUMENT

6. The Government acknowledges that the FBI in this case participated in a joint investigation of the accused. It also acknowledges that the DOJ is closely aligned, in that “The Government collaborated with the federal prosecutors within the DOJ during the accused’s investigation.” *Id.* p. 4. In such circumstances—where the requested discovery is in the possession of an entity that conducted a joint investigation or an entity that is closely aligned with the prosecution—the discovery is deemed to be in the “custody, control, or possession” or military authorities within the meaning of R.C.M. 701(a)(2).

7. R.C.M. 701(a)(2)(A) provides that, upon request of the Defense, the Government shall permit the Defense to inspect:

Any books, papers, documents, photographs, tangible objects, buildings, or places, or copies of portions thereof, *which are within the possession, custody, or control of military authorities*, and which are material to the preparation of the defense or are intended for use by the trial counsel as evidence in the prosecution case-in-chief at trial, or were obtained from or belong to the accused.

(emphasis added). The Government believes that because the FBI and the DOJ are organizations not subject to a military command, then the requested materials are not within the possession, custody, or control of military authorities. *See* Government Response, p. 2 (“the FBI is a subordinate organization to the DOJ, and neither organization is a DOD agency operating under Title 10 status or subject to a military command. Thus, the FBI and DOJ files are not within the possession, custody, or control of military authorities.”). The rule does not speak to whether other *organizations* such as the FBI and DOJ are under military control. Rather, it speaks to whether the books, papers, documents, etc. are within the “possession, custody or control” of military authorities. Thus, the Government misses the critical question posed by the rule: *What materials are considered to be in the “custody, possession or control” of military authorities?*²

8. Whether a document is in the “possession, custody or control” of military authorities is a legal question, not a factual one. *See United States v. Santiago*, 46 F.3d 885, 893 (9th Cir. 1995) (“issue involves a legal determination of the meaning of ‘in the possession of the government.’”). What items are legally considered to be in the “possession, custody or control” of military authorities appears to be a question of first impression in military courts.³ However, the issue has arisen in federal courts under Federal Rule of Criminal Procedure 16, the federal court equivalent to R.C.M. 701(a)(2). *See* Drafter’s Analysis, *Manual for Courts–Martial, Rule 701 Discovery* (“(a) Disclosure by the trial counsel. This subsection is based in part on Fed. R. Crim.

² The Government seems to believe that the relevant question is “What are military authorities?” *See* Government Response, p. 3 (“The prosecution proffers that DOD agencies operating under Title 10 status or subject to a military command are ‘military authorities’”). No one is disputing what military authorities are; the Defense is arguing that certain material, to include the grand jury transcript, is within the “custody, possession or control” of military authorities within the meaning of R.C.M. 701(a)(2).

³ The Defense suspects that the reason this issue has not been litigated is not because the issue is novel, but because military prosecutors are encouraged not to play games with discovery, and thereby routinely turn over to the Defense all the evidence which the Defense requests and to which the prosecutors have access.

P. 16(a), but it provides for additional matters to be provided to the defense. ... [R.C.M. 701(a)(2)] parallels Fed. R. Crim. P. 16(a)(1)(C) and (D)"); *United States v. Stone*, 40 M.J. 420, 423 n.1. (C.M.A. 1994) (when discussing R.C.M. 701(a)(2), noting that "a similar right to discovery [is] provided in Fed. R. Crim. P. 16...."). Rule 16(a)(1)(C) reads as follows:

Upon request of the defendant the government shall permit the defendant to inspect and copy or photograph books, papers, documents, photographs, tangible objects, buildings or places, or copies or portions thereof, *which are within the possession, custody or control of the government*, and which are material to the preparation of the defendant's defense or are intended for use by the government as evidence in chief at trial, or were obtained from or belong to the defendant.

Fed. R. Crim. P. 16(a)(1)(C)(emphasis added). Thus, the language of the two rules is identical, except that the federal rules use the term "government" instead of "military authorities." The term "government" under Rule 16 is synonymous with "prosecution" or "trial counsel." See *United States v. Brazel*, 102 F.3d 1120, 1150 (11th Cir. 1997) ("Binding precedent has construed the term 'government' in Rule 16(a)(1) to refer to the 'defendant's adversary, the prosecution,' given the 'repeated references to the attorney for the government in 16(a)(1)(A), (B) and (D) and 16(a)(2),' and language in 16(a)(1)(C) referring to papers and documents 'intended for use by the government as evidence in chief at the trial.'"). Thus, under Rule 16, the prosecution has the obligation to turn over specifically requested items in "the government's" (i.e. prosecution's) possession, custody and control. R.C.M. 701(a)(2) is intended to be analogous. See Drafter's Analysis, *Manual for Courts-Martial, Rule 701 Discovery* ("[R.C.M. 701(a)(2)] parallels Fed. R. Crim. P. 16(a)(1)(C) and (D)"). The difference is that R.C.M. 701(a)(2) is intended to be broader than its federal counterpart, in that it requires that the Government turn over not only evidence which is within trial counsel's control, but *also* in the control of military authorities generally.⁴ However, the key under both of these rules is determining when a given item is considered to be within a prosecutor's "custody, possession or control." Since military courts have not addressed this issue directly, federal court precedent is instructive in determining how the phrase "custody, possession or control" under R.C.M. 701(a)(2) should be interpreted.

A. Federal Precedent on the Meaning of "Possession, Custody and Control"

- i) Documents are in the "Possession, Custody or Control" of the Government where the Prosecution has Knowledge of, or Access to, the Documents

9. A number of federal courts have accepted that documents are in the "possession, custody or control" of the government for the purposes of Rule 16 where the prosecution had knowledge of, or access to, the documents in question.

10. In *United States v. Libby*, 429 F. Supp. 2d 1 (D.D.C. 2006), for instance, the defendant sought documents that were not in the physical possession of the prosecutor. Rather, they were

⁴ To avoid confusion, it is helpful to read R.C.M. 701(a)(2) as referring to matters within the custody, possession, or control of either trial counsel or military authorities. In this way, it parallels Rule 16, except that it allows for more generous disclosure, in that it includes items within military control as well.

in the physical possession of the White House, more specifically the Office of the Vice President ("OVP") and/or the CIA. The prosecution resisted producing these documents on the basis that they were not in the custody, possession or control of the government within the meaning of Rule 16:

The Special Counsel, however, posits that his office is not obligated, under Rule 16, to search for discoverable documents in the OVP or at the CIA. With regard to the CIA, the Special Counsel contends that the agency did not participate in the grand jury investigation that led to the indictment in this case, but rather has the "status" of nothing more than a "witness" in the investigation. As such, the Special Counsel avers that the CIA is not aligned with the prosecution. Similarly, the Special Counsel argues that the President's directive for White House employees to cooperate with the investigation does not align the OVP with the prosecution because the OVP did not join in the investigation, but merely provided responsive documents to the Office of Special Counsel upon request. The Special Counsel also notes that the President's directive did not provide the Office of Special Counsel with complete access to documents contained in the OVP. Accordingly, the Special Counsel alleges that the documents responsive to the defendant's requests are not "within the possession, custody, or control of the government" as envisioned by Rule 16.

Id. at 9 (internal citations omitted). The court disagreed, holding that the items were discoverable under Rule 16 because the Special Counsel had knowledge of, and access to, the relevant documents requested by the Defense. The court stated:

The Office of Special Counsel has therefore sought and received a variety of documents from both the OVP and the CIA. It was well aware at the outset of this investigation that both of these entities had documents pertinent to the investigation. Moreover, there can be little doubt that upon the Office of Special Counsel's requests, there has been a rather free flow of documents to that Office from both the OVP and the CIA, which have then been used to investigate the alleged unauthorized disclosure of classified information and which were used as the basis for obtaining the indictment in this case. These entities have therefore contributed significantly to the investigation, and without their contribution it is unlikely that the indictment in this case would ever have been secured. Thus, this Court concludes that it has been established that the Office of Special Counsel has knowledge of and access to the documents responsive to the defendant's requests for Rule 16 purposes. Moreover, based upon the nature of the relationship between the Office of Special Counsel and the OVP and the CIA, this Court must conclude that these entities are closely aligned with the prosecution. To hold otherwise, would permit the Office of Special Counsel access to a plethora of documents from the OVP and CIA, which are likely essential to the prosecution of this case, but leave other documents with these entities that are purportedly beyond the Special Counsel's reach, but which are nonetheless material to the preparation of the defense. Such a result would clearly conflict with the purpose and spirit of the rules governing discovery in criminal cases. Accordingly,

because the Office of Special Counsel has benefitted from the cooperation of the White House [and the CIA], ... he cannot now, in fairness, be permitted to disclaim all responsibility for obtaining Presidential [and CIA] documents that are material to the preparation of the defense.

Id. at 11. Thus, because the government in *Libby* had knowledge of, and access to, the documents in question, it could not then resist producing them to the defendant by claiming that they were not in the possession, custody or control of the government.

11. Similarly, in *United States v. Santiago*, the Ninth Circuit found “no [] requirement” that the agency in technical possession of the documents had to have participated in the investigation of the offense in order for the documents to be considered in the possession, custody or control of the government. *United States v. Santiago*, 46 F.3d 885, 893-94 (9th Cir. 1995). Rather, the *Santiago* court held that because the prosecution had “knowledge of and access to the inmate files held by the Bureau of Prisons” the information was discoverable under Rule 16. *Id.* at 894. The court continued:

Unlike cases in which the government lacked any inkling that the documents at issue existed, the prosecution certainly knew that prison files for the inmate witnesses existed. Moreover, because the government was able to obtain Santiago’s prison file from the Bureau of Prisons, it cannot deny that it also had access to the files of other inmates. As a general matter, the fact that the Bureau of Prisons and the United States Attorney’s Offices are both branches of the Department of Justice would facilitate access by federal prosecutors to prison files.

Id. (internal citations omitted).

12. Likewise, in *United States v. Giffen*, 379 F.Supp.2d 337 (S.D.N.Y. 2004), the defendant sought documents (including classified documents) which were in the possession of aligned agencies, including the CIA and the Department of State. The prosecution resisted producing those documents to the defendant under Rule 16 on the basis that they were not within the prosecutor’s direct control. *Id.* at 342. The court found the prosecution’s position unpersuasive, stating that “documents that the government has reviewed or has access to must be provided to aid a defendant in preparing his defense.” *Id.* at 343. Accordingly, because “[t]he Government acknowledges that it has reviewed documents related to [the defendant] at the CIA and the Department of State during the course of its investigation [] [the defendant] is entitled to review those classified document to assess the viability of a public authority defense.” *Id.* See also *United States v. Poindexter*, 727 F.Supp. 1470, 1478 (D.D.C. 1989) (“In this case, the Independent Counsel has had access in the course of its investigation to extensive quantities of White House documents, including some documents held by the former President and Vice President. He has benefitted from the cooperation of the White House in this area, and he cannot now, in fairness, be permitted to disclaim all responsibility for obtaining Presidential documents that are material to the preparation of the defense”).

13. The policy rationale behind the requirement that Rule 16 be interpreted to cover information that the government has access to or knowledge of is articulated in *United States v. Trevino*, 556 F.2d 1265 (5th Cir. 1977):

Certainly the prosecutor would not be allowed to avoid disclosure of evidence by the simple expedient of leaving relevant evidence to repose in the hands of another agency while utilizing his access to it in preparing his case for trial; such evidence is plainly within his Rule 16 "control."

Id. at 1272. See also *United States v. Robertson*, 634 F.Supp. 1020, 1025 (E.D. Cal. 1986) ("limiting 'government' to the prosecution alone unfairly allows the government access to documents without making them available to the defense."). In other words, if the rule were read to cover only documents in the technical possession, custody or control of the government, it would create a perverse incentive for prosecutors to "stash away" relevant evidence with aligned or cooperating agencies. See *United States v. Poindexter*, 727 F.Supp. 1470, 1477 (D.D.C. 1989) ("Courts have in the main been more concerned with fairness to the defendant, on the one hand, and the government's ease of access to the documents sought, on the other, than with the issue whether the documents are actually within the physical possession of the prosecutor."). Clearly, where the government has knowledge of, or access to, an item specifically requested by the Defense, it cannot evade its discovery obligations by claiming that the evidence is not in its possession, custody or control.

ii) Documents are in the "Possession, Custody or Control" of the Government where the Documents are held by an Agency that Participated in a Joint Investigation or by an Agency that is Closely Aligned with the Prosecution

14. It is well-established under federal law that documents held by an agency that is jointly investigating the defendant are in the "possession, custody or control" of the government for the purposes of Rule 16. See e.g. *United States v. Upton*, 856 F.Supp. 727, 749-50 (E.D.N.Y.1994) ("The key to the analysis ... is the level of involvement between the United States Attorney's Office and the other agencies. ... The inquiry is not whether the United States Attorney's Office physically possesses the discovery material; the inquiry is the extent to which there was a *joint investigation* with another agency."); *United States v. McDavid*, 2007 WL 926664, *3 (E.D. Cal.) (court held that "materials are subject to [Rule 16] if the prosecutor has knowledge of or access to them or if they are maintained by an agency involved in the investigation."); *United States v. Johnson*, 2011 WL 4729966, *2 (N.D. Ohio) ("The disclosure requirements [under Rule 16(a)(1)(E)], however, apply not only to the information in the prosecutor's own files, but also to information held by 'the law enforcement agency investigating the offense.'"); *United States v. Holihan*, 236 F.Supp.2d 255, 260 (W.D.N.Y. 2002) ("the prosecutor alone is responsible for ensuring that Defendant is provided with information discoverable under Rule 16, including information that is in the possession of other government agencies participating in the investigation."); *United States v. Microtek International*, 74 F.Supp.2d 1019, 1020 (D. Ore. 1999) (responses to public inquiries are within the control of the government because the Department of Commerce was involved in the investigation of this case); *United States v. Zuno-Arce*, 44 F.3d 1420, 1427 (9th Cir.1995) (prosecutor is "deemed to have knowledge of and

access to anything in the custody or control of any federal agency participating in the same investigation of the defendant.”).

15. It is also well-established that documents that are in the possession of a closely aligned or cooperating agency are deemed to be in the “possession, custody or control” of the government for the purposes of Rule 16. In other words, by virtue of the close relationship between the prosecution and the aligned/cooperating agency, the government has constructive possession, custody or control of the documents. See, e.g., *United States v. Bryant*, 439 F.2d 642, 650 (D.C. Cir. 1971) (tape recording of undercover drug deal with defendant, taken by agents of the Bureau of Narcotics and Dangerous Drugs, was discoverable under Rule 16(a)(1) because “government” may include both the prosecution and an aligned agency); *United States v. NYNEX Corp.*, 781 F.Supp. 19, 25 (D.D.C.1991) (holding that prosecution must produce materials possessed by other federal agencies allied with the prosecution). Thus, where organizations or agencies have engaged in a joint investigation with the prosecution or are closely aligned with the prosecution, the requested items are considered to be in the possession, custody and control of the government within the meaning of Rule 16.

B. Application of Federal Precedent to Interpret “Possession, Custody or Control” in the Instant Case

16. It is clear that under federal law, a prosecutor cannot evade his discovery obligations under the federal equivalent to R.C.M. 701(a)(2) simply by saying that the requested information is not in the possession, custody or control of the government. Instead, the prosecutor is required to either turn over material which: i) he has access to or knowledge of; or ii) is held by agencies that participated in a joint investigation of the accused or by agencies that are closely aligned with the prosecution.

17. In this case, the Government has stated that the “Federal Bureau of Investigation (FBI) ... participated in the joint investigation of the accused.” Government Response, p. 1. Accordingly, any specifically-requested evidence from the FBI’s law enforcement files, including the grand jury transcript, must be turned over under R.C.M. 701(a)(2) as being in the “possession, custody or control” of military authorities.⁵ In fact, the Government has already provided information from the FBI investigation to the Defense in discovery. Thus, the FBI files are clearly in the Government’s possession, custody and control. Why is the Government arbitrarily drawing the line at the grand jury testimony? Why is the grand jury testimony not in the Government’s possession, custody and control, when the other FBI files are?

18. R.C.M. 701(a)(2) must be interpreted to include information that is technically in the hands of a joint investigative agency or any other closely aligned agency. Otherwise, the trial counsel “would [] be allowed to avoid disclosure of evidence by ... leaving relevant evidence to repose in the hands of another agency while utilizing his access to it in preparing his case for trial; such

⁵ The Defense is not clear on exactly which entity, FBI or DOJ, the Government claims is in possession of the grand jury transcript. If the grand jury transcript is within the DOJ, the Court should nonetheless order its production as the DOJ is a closely aligned agency. See Government Response, p. 4 (“The prosecution collaborated with the federal prosecutors within the DOJ during the accused’s investigation”).

evidence is plainly within his Rule 16 ‘control.’” *United States v. Trevino*, 556 F.2d 1265, 1272 (5th Cir. 1977). Such is clearly the case with much of the discovery sought by the defense to date, including the grand jury transcript.

19. If R.C.M. 701(a)(2) were not interpreted in line with federal case law, all an Army prosecutor would need to do to evade his R.C.M. 701(a)(2) discovery obligations would be to involve aligned or cooperating agencies in the case and then ensure that these agencies kept the evidence that the prosecutors did not want disclosed in its entirety.⁶ *United States v. Poindexter*, 727 F.Supp. 1470, 1478 (D.D.C. 1989) (“several courts have noted that a prosecutor who has had access to documents in other agencies in the course of his investigation cannot avoid his discovery obligations by selectively leaving the materials with the agency once he has reviewed them.”). This does not comport with the spirit of R.C.M. 701(a)(2), nor the letter of Rule 701(a)(2), properly construed. See also Article 46, UCMJ (“The trial counsel, the defense counsel, and the court-martial shall have equal opportunity to obtain witnesses and other evidence in accordance with such regulations as the President may prescribe.”).

20. Although there is no military case directly on point, the Court of Military Appeals has recognized that evidence outside the physical possession of the military might nonetheless be within the “possession, custody or control of military authorities.” In *United States v. Charles*, 40 M.J. 414 (C.M.A. 1994), the issue turned on whether certain personnel files related to two civilian state police officers should have been disclosed pursuant to either R.C.M. 701(a)(2) or *Brady*. The military judge in that case had denied the defense access to the civilian personnel files after an *in camera* review; the personnel files were then marked as an appellate exhibit, but subsequently lost. On appeal, the Court of Military review analyzed whether the non-disclosure of the (now lost) records under R.C.M. 701(a)(2) denied the accused his right to appellate review. It concluded that it did not and affirmed the conviction. The Court of Military Appeals framed the issue as whether “appellant had the right to appeal a judge’s decision denying the requested records under R.C.M. 701(a)(2)(A) because they were not ‘material to the preparation of the defense’.” *Id.* at 417. The key, for these purposes, is that both the Court of Military Review and the Court of Military Appeals considered the discoverability of civilian police officer personnel files under R.C.M. 701(a)(2)(A). Clearly, the personnel records of state police officers are not technically in the possession, custody or control of military authorities. State police officers are not, in the Government’s words, operating under Title 10 status or subject to a military command. However, given what was (presumably) some close alignment between the state police and the military authorities in this particular case, these records were properly considered under the R.C.M. 701(a)(2) standard. See also *United States v. Williams*, 2005 WL 3215323 (2005)(unpublished)(in response to a defense discovery request for U.S. customs documents in a case where charges stemmed from wrongful importation of a drug, the court referenced R.C.M. 701(a)(2); while the court ultimately denied discovery, noting that the requested documents would have no effect on resolution of the relevant issues, the court did not state that such customs documents were not in the possession, custody or control of military authorities). Military courts thus recognize that discovery obligations under R.C.M. 701(a)(2) are broader than what may physically be in the possession, custody or control of military authorities.

⁶ The Defense recognizes, of course, that the Government would still have an obligation under *Brady* to produce favorable evidence.

21. R.C.M. 701(a)(2) must be read consistently with federal case law to include documents that are maintained or held by agencies that are jointly investigating the accused or agencies that are closely aligned with the prosecution. If it were not so read, then defendants in federal cases would benefit from much broader discovery rights than their military counterparts, as those defendants would have access under Rule 16(a)(1)(C) to documents of agencies involved in joint investigations or agencies that are closely aligned with the prosecution, while military accuseds would not. This, in turn, could not be reconciled with the repeated statements of military courts that military discovery is much broader than that available in civilian courts. See *United States v. Hart*, 29 M.J. 407, 410 (C.M.A. 1990) (“[D]iscovery available to the accused in courts-martial is broader than the discovery rights granted to most civilian defendants.”); *United States v. Guthrie*, 53 M.J. 103, 105 (C.A.A.F. 2000) (“Discovery in military practice is open, broad, liberal, and generous.”); *United States v. Simmons*, 38 M.J. 376, 380 (C.M.A. 1993) (“Congress intended more generous discovery to be available for military accused.”); *United States v. Killebrew*, 9 M.J. 154, 159 (C.M.A. 1980) (“Military law has long been more liberal than its civilian counterpart in disclosing the government’s case to the accused and in granting discovery rights.”); *United States v. Adens*, 56 M.J. 724, 731 (A. Ct. Crim. App. 2002) (“The military criminal justice system contains much broader rights of discovery than is available under the Constitution or in most civilian jurisdictions.”).

CONCLUSION

22. In accordance with the above, the Defense requests that the Court order the entire grand jury proceedings in relation to PFC Manning or Wikileaks to be produced to the Defense, or alternatively, that it be produced for *in camera* review to determine whether the evidence is discoverable under R.C.M. 701(a)(2) as being material to the preparation of the defense. If the Court concludes that grand jury testimony is not within the possession, custody or control of military authorities, the Defense still requests that the Court order production of the entire grand jury investigation under the “relevant and necessary” standard under R.C.M. 703.

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

18 April 2012

MEMORANDUM FOR RECORD


SUBJECT: Security Expert Review of Defense Motions

1. I hereby certify that I have reviewed the following Defense motion for the presence of classified information:

a) Defense Reply to Prosecution Response to Defense Request for Partial Reconsideration of Discovery Ruling

I do not believe that this motion contains classified information or information that a reasonable person could believe to be classified.

2. The point of contact for this memorandum is the undersigned at (703) 428-4340.



CASSIUS HALL
IS Division
INSCOM G2

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, xxx-xx-[REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

**DEFENSE RENEWAL OF
MOTION FOR PARTICULARS**

DATED: 6 April 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, moves this court, pursuant to R.C.M. 906(b)(6) and the Fifth, Sixth and Eighth Amendments to the United States Constitution to direct the Government to file the requested particulars for the 18 U.S.C. §641 offense.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. As the moving party, the Defense has the burden of persuasion. R.C.M. 905(c)(2). The burden of proof is by a preponderance of the evidence. R.C.M. 905(c)(1).

WITNESSES/EVIDENCE

3. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this court to consider the referred charge sheet in support of its motion.

LEGAL AUTHORITY AND ARGUMENT

4. The Government has opposed the Defense's request for particulars on whether the Government alleges that PFC Manning "stole" or "converted" under 18 U.S.C. §641. The Court ordered that the Defense provide the Government with authority that showed there was a difference between "stealing" and "converting" within the meaning of section 641. On 19 March 2012, the Defense sent the following email to the Court and the Government:

At the last 39(a), the Court requested the Defense to provide cases concerning the terms steal, purloin, and convert with regards to 18 U.S.C. §641. In this case, the Government

does not allege embezzlement. Instead, the Government alleges steal, purloin, or knowingly convert. Based upon the charged specification:

a) Steal: To steal property means to take someone else's property without the owner's consent with the intent to permanently deprive the owner of the value of that property. *Morrisette v. United States*, 342 U.S. 246, 270-71 (1952) ("Probably every stealing is a conversion, but certainly not every knowing conversion is a stealing. 'To steal means to take away from one in lawful possession without right with the intention to keep wrongfully.'") (citations omitted.)

b) Purloin: To purloin is to steal with the element of stealth, that is, to take by stealth someone else's property without the owner's consent with the intent to permanently deprive the owner of the value of that property. *Morrisette v. United States*, 342 U.S. 246, 270 (1952).

c) Conversion: To knowingly convert property means to use the property in an unauthorized manner in a way which seriously and substantially interfered with the government's use of the property, knowing that the property belonged to the United States, and knowing that such use was unauthorized. *Morrisette v. United States*, 342 U.S. 246, 271-72 (1952).

I believe that I understood the Government's position to be that there was no difference between steal and purloin. Thus, we are only dealing with steal or knowingly convert. Given the Supreme Court's clear pronouncement that there is a distinction between stealing and knowingly converting, the Defense requests that the Government provide clarification as to which theory it is alleging.

5. The Government did not respond to this email. Almost two weeks later, the Defense sent another email to the Government asking if it was planning on responding. The Government responded as follows:

In reference to the below email, we agree that under *Morrisette* the Court determined there may be slight variances between what constitutes stealing and knowing conversion. However, each federal circuits' jury instructions are different and some circuits treat the two similarly. We still do not believe the government is required to specify which theory we are alleging. The accused is on notice of both theories. This is still a matter best left for instructions. [Email from MAJ Fein, 2 April, 2012].

6. The Government acknowledges that the U.S. Supreme Court has determined that there is a difference between "stealing" and "converting" under section 641. However, according to the Government, because some circuits' pattern jury instructions treat the offenses similarly, it will not provide the requested particulars.

7. The Defense does not understand the Government's position. The Supreme Court has said that "stealing" and "converting" are two different offenses under section 641. See *Morrisette*, *supra*. But because the Government believes that some unspecified boilerplate jury instructions treat the offenses similarly, this is cause to refuse to provide the requested particulars? Contrary

to the Government's belief, the instructions don't inform the law; rather, the law informs the instructions.

CONCLUSION

8. In light of the Government's (appropriate) concession that stealing and converting are two different things, the Defense requests that the Court order the Government to provide the requested particulars.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. Coombs', with a stylized flourish at the end.

DAVID EDWARD COOMBS
Civilian Defense Counsel

From: David Coombs
To: Lind, Denise R COL MIL USA OTJAG
Cc: "Kemkes, Matthew J MAJ USARMY (US)"; "Bouchard, Paul R CPT USARMY (US)"; "Santiago, Melissa S CW2 USARMY (US)"; Morrow III, JoDean CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H CPT USA JFHQ-NCR/MDW SJA; Ford, Arthur D CW2 USA JFHQ-NCR/MDW SJA; ashden.fein@us.army.mil; Williams, Patricia CTV JFHQ-NCR/MDW SJA; Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA; dashawn.jefferson@conus.army.mil
Subject: Renewal of Bill of Particulars Motion
Date: Friday, April 06, 2012 4:00:11 PM
Attachments: [Def Bill of Particulars - renewal.pdf](#)
[Def Bill of Particulars - renewal.doc](#)

Ma'am,

Please find attached the Defense's Renewal of Motion for Particulars.

v/r
David

David E. Coombs, Esq.
Law Office of David E. Coombs
11 South Angell Street, #317
Providence, RI 02906
Toll Free: 1-800-588-4156
Local: (508) 689-4616
Fax: (508) 689-9282
coombs@armycourt martialdefense.com
www.armycourt martialdefense.com

Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

**GOVERNMENT REPLY
TO DEFENSE RENEWAL OF
MOTION FOR PARTICULARS**

17 April 2012

RELIEF SOUGHT

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny the defense renewal of its motion for particulars.

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the defense has the burden of persuasion on any factual issue the resolution of which is necessary to decide the motion. RCM 905(c)(2). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

WITNESSES/EVIDENCE


The United States requests the Court consider the referred charge sheet.

LEGAL AUTHORITY AND ARGUMENT


The United States is not required to clarify the specific theory it is alleging with respect to Specifications 4, 6, 8, 12, and 16 of Charge II. The defense is on notice that the accused stole, purloined, or knowingly converted property belonging to the United States. The United States has not charged the accused with different offenses in one specification; merely alternative ways of committing the same offense. *See* 18 U.S.C. §641. In this case, the defense is using its request for particulars to restrict the Government's proof relating to the methods of committing the underlying offense. A bill of particulars is not appropriate when used to restrict the Government's proof at trial. *See* RCM 906(b)(6) discussion.

CONCLUSION

For the reasons stated above, the United States requests this Court DENY the defense renewal of its motion for particulars.


JODEAN MORROW
CPT, JA
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 17 April 2012.


JODEAN MORROW
CPT, JA
Trial Counsel

From: Fein, Ashden MAJ USA JFHO-NCR/MDW SJA
To: Lind, Denise R COL MIL USA OTJAG
Cc: David Coombs; "Tooman, Joshua J CPT USARMY (US)"; melissa.s.santiago.mil@mail.mil; Morrow III, JoDean, CPT USA JFHO-NCR/MDW SJA; Overgaard, Angel M, CPT USA JFHO-NCR/MDW SJA; Whyte, Jeffrey H, CPT USA JFHO-NCR/MDW SJA; VonElten, Alexander S, 1LT USA JFHO-NCR/MDW SJA; Ford, Arthur D, CW2 USA JFHO-NCR/MDW SJA; Williams, Patricia CIV JFHO-NCR/MDW SJA; Jefferson, DaShawn MSG MIL USA OTJAG
Bcc: Bradley, Princeton L, SGT USA JFHO-NCR/MDW SJA; Felto, Beatriz SGT USA JFHO-NCR/MDW SJA; Parra, Jairo A, CW2 USA JFHO-NCR/MDW SJA; Waybriht, Daniel W, SGT USA JFHO-NCR/MDW SJA; Haberland, John CPT USA Regimental Judge Advocate
Subject: Response & Reply
Date: Tuesday, April 17, 2012 8:47:00 PM
Attachments: 120417-Government Response to Discovery Reconsideration.docx
120417-Government Response to Discovery Reconsideration.pdf
120417-Reply to Motion to Renew BoP.docx
120417-Reply to Motion to Renew BoP.pdf

Ma'am,

Attached to this email are the following documents:

1. Government Response to Discovery Reconsideration-Grand Jury
2. Government Reply to Motion to Renew Bill of Particulars

v/r
MAJ Fein

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army, xxx-xx-)

Headquarters and Headquarters Company, U.S.)

Army Garrison, Joint Base Myer-Henderson Hall,)
Fort Myer, VA 22211)

**DEFENSE RENEWAL OF
MOTION TO COMPEL
DISCOVERY OF COMPUTERS**

DATED: 30 March 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by counsel, pursuant to R.C.M. 701(a)(6) and 701(2)(A) and applicable case law, requests this Court to order the Government to conduct searches on the relevant computers as outlined in this motion. If the Court does not grant this Order, the Defense requests specific findings of fact and law on the record.

FACTS

2. On 23 March 2012, the Court granted the Defense Motion to Compel Discovery in part with regard to the 14 hard drives from the Tactical Sensitive Compartmented Information Facility (T-SCIF) and the Tactical Operations Center (TOC) of Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division, Forward Operating Base (FOB) Hammer, Iraq. The Court Ordered the Government to immediately cause an inspection of the 14 hard drives for the presence of "Wget, M-IRC Chat, Google Earth, movies, games, music and any other specifically requested program from the Defense." See Ruling: Defense Motion to Compel Discovery, p. 11.

3. The Defense, in consultation with its computer forensic experts, proposed a process that would accurately identify any unauthorized music, movies, games, or other programs. The process could be easily completed within a matter of a few days and would not reveal the content of any file. Thus, the information revealed would not be classified, and would not necessitate a review by any Original Classification Authority (OCA).

4. The process recommended by the Defense involved the Government's forensic experts providing the Defense with an EnCase Folder Structure in .rtf format that includes the filenames within each of the following folders for every identified user profile on each hard drive:

- a. Program Files;

b. User Profile Storage regarding: Music, Games, Pictures, Local Settings\Application Data; (the Defense has eliminated any reference to "documents" and "etc." in order to avoid any confusion by the Government);

c. Windows\Prefetch; and

d. The following four paths¹: (1) Documents and Settings\<username>\Local Settings\Application Data; (2) Documents and Settings\<username>\Application Data; (3) Users\<username>\AppData\Local; and (4) Users\<username>\AppData\Roaming.

5. The Government opposed the Defense request stating that the list of file names would likely also list classified information because many filenames have actual classified information in the names, such as the ones the accused has been charged with compromising. [Email from MAJ Ashden Fein, March 26]. The Government also stated that its position is that the Defense should be able to at least articulate what unauthorized software it believes is on the hard drives, "otherwise this is a classic fishing expedition for classified information." *Id.* With a Defense provided list, the Government stated that its expert could search the drives and determine whether the information is actually on the drive.

6. The Court tentatively ruled that it would not force the Government to identify all programs on the 14 hard drives. The Court's position was based, in part, upon a belief that the Government did not concur with the Defense that the process could easily be accomplished without the need for a lengthy delay.

7. Based upon the concerns of the Court, the Defense contacted its computer forensic experts again and asked if there were an easier process that would eliminate the Government's objections and the Court's concerns. Mr. Trent Struttman, one of the Defense computer forensic experts, suggested an even simpler process. This process will allow the Government to obtain only a list of installed programs. According to Mr. Struttman, the process can be achieved in less than five minutes. The proposed process is as follows:

- a. Load up the case file;
- b. Run the "Case Processor" and select "Windows Initialize Case";
- c. Choose to run the "software" module;
- d. Hit "OK" and then wait for the process to finish.

8. Mr. Struttman maintains that the Case Processor should take less than 30 seconds to complete its task. Once the task is completed, the user simply needs to go to the bookmarks tab. Within the bookmarks tab, one will see a "Software Info" folder that the Case Processor has just created. The user then needs to hit the "Report Tab" and export the results to a RTF list. This

¹ Each identified path was not specifically detailed in the Defense's original request, but is now being identified in order to be responsive to the Government's concern of revealing classified information. The listed paths will avoid any classified documents or classified content.

would then complete the entire process. Once complete, one would have a complete and accurate list of all software (and only the software) on the computer by name without any other information. This process would only provide a list of software. The Government would then need to separately identify any unauthorized music or movies.

WITNESSES/EVIDENCE

9. If the Government does not stipulate that the above process is accurate, the Defense requests the testimony of Mr. Trent Struttman for the purposes of this motion.

ARGUMENT

10. The Defense believes it is entitled to discovery of the relevant computers under R.C.M. 701(2)(A) as being “tangible objects ... which are within the possession, custody or control of military authorities, and which are material to the preparation of the defense.” The Defense also maintains that if the computers contain the software that the Defense has reason to believe they contain, then this information would be classic *Brady* material that the Government is obligated to disclose to the Defense under R.C.M. 701(a)(6).

11. While the Defense believes that it is entitled to inspect the actual computers (or a digital image thereof), in the interest of expediency, the Defense is amenable to having the Government perform a meaningful search of the computers for the requested information. As submitted to the Court, the Defense proposes that the Government’s forensic experts follow a simple process that will yield a list of program/software names. This, in turn, can be compared against the list of 94 authorized programs to determine how pervasive the practice of adding of “unauthorized” software was in the T-SCIF and TOC.

12. The Defense’s tentative theory is that all or most soldiers in the SCIF had unauthorized software on their computers (e.g., M-IRC Chat, Google Earth, Wget, movies, music, games, etc.). This is amply supported by the Article 32 testimony. The Defense intends to show that the practice of adding “unauthorized” software was so pervasive that, in effect, all “unauthorized” programs were implicitly or explicitly authorized. As aptly stated in this Court’s ruling, the Defense’s theory is that “the information is relevant to establish the defense theory that the addition of software not on the approve list of authorized software was authorized by the accused’s chain of command through the practice of condoning and implicitly or explicitly approving the additions of such software.” (Ruling: Defense Motion to Compel Discovery, p. 4). Simply because the Government does not believe this is a viable defense does not mean that the Defense should not be able to pursue it and advance it at trial, if there is evidence to support it.²

² The Court alludes to the fact that the “Defense has evidence from the Article 32 witnesses to further the Defense’s theory” – thus suggesting that a full search of the computers is not necessary. While the evidence at the Article 32 hearing certainly supports the Defense’s theory, it does not establish just how widespread the practice was.

13. The Defense also believes that if the search yields the expected results (i.e. that it was common for soldiers to add unauthorized software), this is classic *Brady* material under R.C.M. 701(a)(6). The Defense would argue that this would reasonably tend to negate or reduce guilt for the charged offenses related to unauthorized software. At a very minimum, it would reasonably tend to reduce punishment. If it can be shown that every other soldier in PFC Manning's unit also downloaded software that was not on the approved list, this would certainly bear on the punishment that PFC Manning should receive for these particular offenses (which carry with them a maximum period of 4 years of confinement combined).

14. The Defense believes that if PFC Manning had only been charged with the offense of adding unauthorized software to a government computer, the Government would not be maintaining the position it is. The Government cannot fulfill its *Brady* obligations simply by turning over evidence that this favorable to the Defense in that it tends to reduce guilt or punishment of the *more serious* offenses. *Brady* applies equally to all offenses.

15. There is clear evidence that many soldiers added "unauthorized" software to computers. Now that the Government has this knowledge, it cannot simply ignore it. It has the independent obligation to search the computers to turn over evidence that falls within R.C.M. 701(a)(6). Moreover, the request for a list of software programs on the relevant computer is squarely within the parameters of R.C.M. 701(2)(A), which provides that all tangible items in the Government's possession, custody or control must be turned over if they are "material to the preparation of the Defense." As argued in the Motion to Dismiss, the standard of materiality is not a high one. *See, e.g., United States v. Roberts* 59 M.J. 323 (C.A.A.F. 2004) ("The defense had a right to this information because it was relevant to SA M's credibility and was therefore material to the preparation of the defense for purposes of the Government's obligation to disclose under R.C.M. 701(a)(2)(A).").

16. The Court ruled on 23 March 2010 that a complete search of the hard-drives was not material to the preparation of the defense for the charged specifications. However, the Court directed the Government to "search each of the 14 hard drives [for] Wget, M-IRC Chat, Google Earth, moves, games, music, and any other specifically requested program from the Defense." *See* Ruling: Defense Motion to Compel Discovery, p. 11. When the Defense consulted with its computer experts, it learned that this process was not likely to yield meaningful results in terms of getting access to the information sought – i.e. exactly how pervasive was the practice of adding unauthorized software in the SCIF? The Defense's expert proposed an alternative means of searching the relevant computers which would be minimally cumbersome for the Government and would yield the results sought by the Defense.

17. The Government has resisted this proposed approach, indicating instead that the Defense must submit a list of software programs that the Government will then specifically search for.

Moreover, it allows the Government to undercut the Defense's theory by calling rebuttal witnesses – all while having access the *actual forensic* results and not disclosing them to the Defense. In short, the Government should not be able to remain willfully blind and then call rebuttal witnesses to suggest that the practice was not widespread when it has evidence in its possession that could verify the facts either way. Further, unit witnesses are not likely to be forthcoming with whether they did, in fact, add unauthorized software to computers as this would incriminate them and subject them to criminal prosecution for violating a lawful general regulation.

Unfortunately, this misses the point of the entire discovery request. The point was to see how many other unauthorized software programs were found on the computers in the SCIF. If the Defense submits a list with, say, 50 different software programs and 5 of them are found on the relevant hard drives, this does not prove anything. It simply proves that these 5 random software programs were on some or all of the hard drives. It does not speak to the pervasiveness of the practice of adding authorized programs to government computers.

18. The Defense's computer experts have indicated that there are over 5 billion records of software in the Global Software Registry. To prepare a list that the Government will then look for is like playing a game of "Battleship" where the Defense has to guess which particular programs a soldier in PFC Manning's SCIF might have downloaded.³ If the Defense guesses correctly, then that might be some proof (however limited) that others downloaded unauthorized software. If the Defense guesses incorrectly, which it is apt to do given the number of software programs out there, this does not prove anything. It simply shows—to use the Battleship analogy—that the Defense has not guessed the right coordinates.

19. The Government further resists performing the search requested by the Defense on the grounds that it is likely to yield classified data.⁴ The Defense has trouble understanding how a screen shot of program/software names will yield classified data. But, to the extent that it does, the Defense has requested that the Government simply redact the classified information and state something to the effect of, "Program X, not on approved software list." The Defense is not interested in the *names* of the programs, or even the *types* of programs—simply the *number* of programs that appear on the hard drives that are not on the approved software list. Additionally, under the process recommended by Mr. Struttman, the concern of the Government is eliminated (based upon the Government's representation during the 802 conference that it was unaware of any classified programs on the DCGS-A computer).

20. The Defense has proposed a simple, common-sense way of proceeding that avoids the potential disclosure of classified information. And yet, the Government inexplicably opposes the request. If the results of the proposed search are favorable, then they are *Brady* material which the Government must disclose. If the results of the search are unfavorable (i.e. no other soldier added software to his/her computer), then that evidence will be helpful to the Government's

³ Battleship is a guessing game involving two players. The game is played on four grids, two for each player. The grids are typically square – usually 10×10 – and the individual squares in the grid are identified by letter and number. On one grid the player arranges ships and records the shots by the opponent. On the other grid the player records his/her own shots. Before play begins, each player arranges a number of ships secretly on the grid for that player. Each ship occupies a number of consecutive squares on the grid, arranged either horizontally or vertically. The number of squares for each ship is determined by the type of the ship. The ships cannot overlap (i.e., only one ship can occupy any given square in the grid). After the ships have been positioned, the game proceeds in a series of rounds. In each round, each player's turn consists of announcing a target square in the opponent's grid which is to be shot at. If a ship occupies the square, then it takes a hit. The player's opponent announces whether or not the shot has hit one of the opponent's ships and then takes a turn. When all of the squares of a ship have been hit, the ship is sunk. After all of one player's ships have been sunk, the game ends and the other player wins. See [http://en.wikipedia.org/wiki/Battleship_\(game\)](http://en.wikipedia.org/wiki/Battleship_(game)).

⁴ The fact that unauthorized program names may hypothetically yield classified information is not a reason to refuse to conduct a *Brady* search or to turn over specifically-requested items pursuant to R.C.M. 701(a)(2). As stated in the Court's order, "*Brady*, RCM 701(a)(2), 701(a)(6), and 701(g) govern discovery of both classified and unclassified information." (Ruling: Defense Motion to Compel Discovery, pg. 10).

prosecution of this offense.⁵ Given this, it is difficult to understand the Government's opposition to the Defense proposal.

CONCLUSION

21. In light of the foregoing, the Defense requests that this Court order the Government to review the hard drives of the 14 computers using either of the methods proposed by the Defense's experts.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. Coombs', with a stylized flourish at the end.

DAVID EDWARD COOMBS
Civilian Defense Counsel

⁵ Such information would also be helpful to the Defense within the meaning of R.C.M. 701(a)(2) in that it may signal to the Defense that, as a trial strategy, this avenue is not worth pursuing.

30 March 2012

MEMORANDUM FOR RECORD

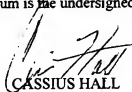
SUBJECT: Security Expert Review of Defense Motions

1. I hereby certify that I have reviewed the following Defense motions for the presence of classified information:

- a) Defense Request for Search Terms of Relevant Computers; and
- b) Defense Renewal of Motion to Compel Discovery of Computers;

I do not believe that either of these motions contains classified information or information that a reasonable person could believe to be classified.

2. The point of contact for this memorandum is the undersigned at (703) 428-4340.


CASSIUS HALL
IS Division
INSCOM G2

30 March 2012

MEMORANDUM FOR RECORD

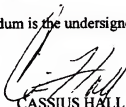
SUBJECT: Security Expert Review of Defense Motions

1. I hereby certify that I have reviewed the following Defense motions for the presence of classified information:

- a) Defense Request for Search Terms of Relevant Computers; and
- b) Defense Renewal of Motion to Compel Discovery of Computers;

I do not believe that either of these motions contains classified information or information that a reasonable person could believe to be classified.

2. The point of contact for this memorandum is the undersigned at (703) 428-4340.



CASSIUS HALL

IS Division

INSCOM G2

From: David Coombs
To: Lind, Denise R COL MIL USA OTJAG
Cc: "Kemkes, Matthew J MAJ USARMY (US)"; "Bouchard, Paul R CPT USARMY (US)"; "Santiago, Melissa S CW2 USARMY (US)"; Morrow III, JoDean, CPT USA JFHQ-NCB/MDW SJA; Overgaard, Angel M, CPT USA JFHQ-NCB/MDW SJA; Whyte, Jeffrey H, CPT USA JFHQ-NCB/MDW SJA; Ford, Arthur D, CW2 USA JFHQ-NCB/MDW SJA; ashden.fein@us.army.mil; "Prather, Jay R CIV (US)"; Williams, Patricia CIV JFHQ-NCB/MDW SJA; Fein, Ashden MAJ USA JFHQ-NCB/MDW SJA
Subject: Search of T-SCIF and TOC Computers
Date: Friday, March 30, 2012 11:05:21 AM
Attachments: Discovery Renewal - Computers.pdf
Def. Program List.pdf
Security Expert Review.pdf

Ma'am,

The Defense has attached the following motions:

- a) Defense Request for Search Terms of Relevant Computers; and
- b) Defense Renewal of Motion to Compel Discovery of Computers.

The Defense has also attached the review of both motions by its security expert - Mr. Cassius Hall.

v/r
David

David E. Coombs, Esq.
Law Office of David E. Coombs
11 South Angell Street, #317
Providence, RI 02906
Toll Free: 1-800-588-4156
Local: (508) 689-4616
Fax: (508) 689-9282
coombs@armycourt martialdefense.com
www.armycourt martialdefense.com

Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, xxx-xx-██████

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

**DEFENSE FORENSIC REQUEST
OF RELEVANT COMPUTERS**

DATED: 26 March 2012

1. The Defense, in consultation with its computer forensic experts, requests the following process be performed in order to facilitate the Court's Order compelling the Government to immediately cause an inspection of 14 hard drives from the Tactical Sensitive Compartmented Information Facility (T-SCIF) and the Tactical Operations Center (TOC) of Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division, Forward Operating Base (FOB) Hammer, Iraq:

a. The Government provides the Court and Defense with a list of the approved programs for the Distributed Common Grounds System – Army (DCGS-A) computer;

b. The Government's forensic experts provide the Defense with an EnCase Folder Structure in .rtf format that includes the filenames within each of the following folders for every identified user profile on each hard drive:

(1) Program Files;

(2) User Profile Storage regarding: Documents, Music, Games, Pictures, Local Settings\Application Data etc.;

(3) Windows\Prefetch

2. The requested process will accurately identify any unauthorized music, movies, games, or other programs. The process will not, however, reveal any content of any file. Thus, the information revealed will not be classified, and will not necessitate a review by any Original Classification Authority (OCA).

3. The above process can easily be completed within a matter of a few days. The process will also eliminate the need for the Government to search each computer for every conceivable form of unauthorized media (music, movies, games and other programs). Moreover, this process avoids the Defense having to guess at what, of the millions of software programs out there, might be found on the relevant computers.

4. The point of contact for this memorandum is the undersigned at (401) 744-3007 or by e-mail at coombs@armycourtmartrialdefense.com.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. Coombs', with a stylized flourish at the end.

DAVID EDWARD COOMBS
Civilian Defense Counsel

30 March 2012

MEMORANDUM FOR RECORD

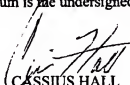
SUBJECT: Security Expert Review of Defense Motions

1. I hereby certify that I have reviewed the following Defense motions for the presence of classified information:

- a) Defense Request for Search Terms of Relevant Computers; and
- b) Defense Renewal of Motion to Compel Discovery of Computers;

I do not believe that either of these motions contains classified information or information that a reasonable person could believe to be classified.

2. The point of contact for this memorandum is the undersigned at (703) 428-4340.


CASSIUS HALL
IS Division
INSCOM G2

30 March 2012

MEMORANDUM FOR RECORD

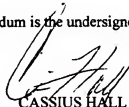
SUBJECT: Security Expert Review of Defense Motions

1. I hereby certify that I have reviewed the following Defense motions for the presence of classified information:

- a) Defense Request for Search Terms of Relevant Computers; and
- b) Defense Renewal of Motion to Compel Discovery of Computers;

I do not believe that either of these motions contains classified information or information that a reasonable person could believe to be classified.

2. The point of contact for this memorandum is the undersigned at (703) 428-4340.



CASSIUS HALL
IS Division
INSCOM G2

From: David Coombs
To: Lind, Denise R COL MIL USA OTJAG
Cc: "Kemkes, Matthew J MAJ USARMY (US)"; "Bouchard, Paul R CPT USARMY (US)"; "Santiago, Melissa S CW2 USARMY (US)"; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M, CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H, CPT USA JFHQ-NCR/MDW SJA; Ford, Arthur D, CW2 USA JFHQ-NCR/MDW SJA; ashden.fein@us.army.mil; "Prather, Jay R CTV (US)"; Williams, Patricia CTV JFHQ-NCR/MDW SJA; Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA
Subject: Search of T-SCIF and TOC Computers
Date: Friday, March 30, 2012 11:05:21 AM
Attachments: Discovery Renewal - Computers.pdf
Def. Program List.pdf
Security Expert Review.pdf

Ma'am,

The Defense has attached the following motions:

- a) Defense Request for Search Terms of Relevant Computers; and
- b) Defense Renewal of Motion to Compel Discovery of Computers.

The Defense has also attached the review of both motions by its security expert - Mr. Cassius Hall.

v/r
David

David E. Coombs, Esq.
Law Office of David E. Coombs
11 South Angell Street, #317
Providence, RI 02906
Toll Free: 1-800-588-4156
Local: (508) 689-4616
Fax: (508) 689-9282
coombs@armycourt martialdefense.com
www.armycourt martialdefense.com

Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.

UNCLASSIFIED//FOUO

**Version Description Document (VDD)
For**

**Basic Analyst Laptop
(BAL)**

**Distributed Common Ground Systems – Army
Software Version 3.1 Patch 3
(DCGS-A V3.1 P3)**

1 October 2009



DCN: 149015, Rev 1

UNCLASSIFIED//FOUO

Revision History

Revision	Date	Page(s)	Para.	Description of Change
Original	February 17, 2009	N/A	N/A	Initial release
1	October 1, 2009	N/A	N/A	Release of new Image with Re partition of Drives, with SQL, Data Base hardening and configuration changes

1.	Scope	1
1.1	Identification.....	1
1.2	System Overview.....	1
1.3	Document Overview.....	1
2.	Referenced Documents	1
3.	Version Description.....	1
3.1	Inventory of Materials Released.....	1
3.2	BAL Media Listing	2
3.3	Software Description.....	2
3.4	Possible Problems and Known Errors.....	6
3.5	Adaptation data.....	7
3.6	Related Documents.....	7
3.6.1	Post Clone Procedures	7
3.6.2	Installation Procedures	7
3.6.3	Technical Bulletins.....	7
3.6.4	Overwatch MFWS Release 6.2	9
3.7	COTS Software Sites	10
3.8	Hardware Description	10

1. Scope

1.1 Identification

This Version Description Document (VDD) describes software release V3.1 P3 being developed at the direction of the Project Manager DCGS-A for use in the DCGS-A V3.1 P3 Basic Analyst Laptops (BALs), which include Dell M90, M6300, and the Alienware (A51M). Two other Client platforms are the Dell M490 Workstation, T5400 Desktop. The BALs, Workstation and Desktop software version will be authorized to process up to Secret Collateral information and connect to the Secret Internet Protocol Router Network (SIPRNET) in accordance with AR 25-2 Information Assurance and Department of Defense (DoD) Instruction 8500.2 Information Assurance (IA) Implementation.

1.2 System Overview

The A51M, M90 and/or M6300 are high-end laptop computers with a 17" monitor capable of displaying high-resolution graphics. The Dell 490 Workstation and T5400 Desktop with the V3.1P3 SW is used within the DCGS-A fixed site baseline. Microsoft Windows XP Professional (Service Pack3) utilized as the operating system. The A51M, M90, M6300, Dell 490 and T5400 provide the Army a client workstation for use by DCGS-A analysts.

Note: The A51M, M90, M6300, Dell 490 and T5400 is classified because of a file change within the Query Tree Multi Functional Work Station (MFWS) Plug-In and the change to the high water marking.

1.3 Document Overview

This VDD documents the release tested and type-accredited with the DCGS-A V3.1 P3 Collateral components in the DCGS-A laboratory environment at Fort Monmouth, NJ, released to the Central Technical Support Facility (CTSF), Fort Hood, TX; and then released to operational users for site accreditation.

2. Referenced Documents

Field Service Engineer (FSE) Training Guide, Part # 3.1.03.1002.C, dated 1 October 2009 prepared by I2WD, Fort Monmouth NJ.

Note: All referenced documents are resident in the Software Engineering Center (SEC) Software Control and Reference Office (SCRO).

3. Version Description

3.1 Inventory of Materials Released

Software for the DCGS-A V3.1 P3 BAL is installed at the Software Integration Lab (SIL) onto the laptop's hard drive. Consequently, no media will be delivered with the DCGS-A V3.1 P3 BAL. All updates are provided through download from digital media.

25 Hard Drives and 3 DVDs containing software and documentation for DCGS-A Version 3.1 P3 is resident in the Software Engineering Center (SEC) Software Control and Reference Office (SCRO) reference on paragraph 3.2. BAL Media Listing.

3.2 BAL Media Listing

CM Control Number	SCRO CINCODE	Date of media	Destination	Created By	Contents	Media Type
DCGS0303	N/A	4-Nov-09	SEC IFS/ SCRO	SEC SCIF	DCGS-A V3 1P3 - M90 and/or M6300, Alienware (A51M), Dell 490 Workstation and T5400 Desktop Client image - Secret	1 HD
DCGS0318	N/A	1-Oct-09	SEC IFS/ SCRO	SEC SCIF	DCGS-A V3 1 P3 - APP1, APP2, IOP, MDC & BALs Image	1 set of 1 HD

3.3 Software Description

The following is a list of DCGS-A V3.1 P3 Client SW detailed software information:

NOTE: The Client SW listed can be loaded on the five platforms that include Dell M90, M6300, A51M, Dell M490 Workstation and the Dell T5400 Desktop. Once the SW is loaded onto the platform, the appropriate drives are loaded. The i2 Analysis Notebook (ANB) is loaded on the system without an active software license, if the user chooses to use ANB; the user will procure the license. The Axis Pro capabilities are in the DCGS-A MFWS V3.1.

BAL Software	Version	Vendor	Function/Component
Acrobat Reader 9	9.1.2	Adobe	PDF file reader
Adobe Flash Player Plug-in	10.0.32.18	Adobe	Adobe Flash is the authoring environment and Flash Player is the virtual machine used to run the Flash files
Adobe Flash Player 10 Active X	10.0.22.87	Adobe	Flash Player
Alert Services Client Runtime (ALTCLT)	4.53.5	Future Skies	Alert Service Application
ArcGIS Desktop	9.2.1500	ESRI	Geospatial data management and presentation
ArcMap	9.2	ESRI	Geospatial data management and presentation
ArcGIS Military Analyst (Military Analyst 9.2 SP2)	9.2.401	ESRI	Geospatial data management and presentation
ArcGIS Military Overlay Editor 9.2 (SP1)	9.2.0.430	ESRI	Geospatial data management and presentation
CECOM_MapShapes	1.00.0000	Overwatch	
Chart Scrapper	7.2.0.1	Novel Application	Data Movement tool

BAL Software	Version	Vendor	Function/Component
C2R	4.70.9	GOTS/PD CS	Address Book Services
C2R Planner	1.00.0000	GOTS/PD CS	Address Book Services
CMP	4.7.0.6	GOTS/PD CS	Common Message Processor
DB Importer	7.1.0	Novel App Inc.	DB Importer
DCGS-A Configuration Assistant	1.3.0 20090504	I2WD	Post clone assistant
DCGS-A MFWS V3.1	6.2.6.1077	Overwatch	Multi function Workstation DCGS-A APP Framework SDK; v 1.7.13
DCGS-A_V3.1_Full	6.2.0.1035	Overwatch	Multi function Workstation
DCGS-A Multimedia Plugin	1.0.0	BAH	Multi function Workstation
DCGS-A Web Folder Plugin	2.0.0	BAH	Multi function Workstation
DCI (DOS Client Interface)	5.1.5.0	Future Skies	
DCGS-A Weather IWEDA Client Tri-Service IWEDA -20061129	6.4.2.8	Army Research Lab	Weather effect decision aid
Digital Topographic Support Systems (DTSS) 9.0 6 Rendering Package	9.0	Northrop Grumman	To provide critical, timely, and accurate digital and hardcopy geospatial information
DIB Client Adapter	1.3	CSP Tech	Installer for the Viper DIB Client Adapter
GeoRover for ArcGIS	3.10.0000	SAIC	Geospatial software product extensions or "plugins" to ArcMap
GeoRover Coordinate Viewer Extension	1.0.2	SAIC	Geospatial
GeoRover Digital Data Tracker Extension	3.2.5	SAIC	Geospatial
GeoRover License Manager	1.1.0	SAIC	Geospatial
GeoRover Locus Track Extension	3.2.4	SAIC	Geospatial
GeoRover Zoom Tools Extension	3.2.4	SAIC	Geospatial
Ground Tactical Communication (GTCS)	4.7.0.9	GOTS/PD CS	Message Transport Protocol

BAL Software	Version	Vendor	Function/Component
Google Earth EC	4.2.205.5730	Google	Virtual globe, map and geographic information
Grid Extractor	1.2		
i2 Analyst Notebook 6	6.055.1022	i2	Link & Timeline Analysis tool w/ graphical representation
i2 Online Link 6	6	i2	i2 Online iLink is a feature of Analyst's Notebook 6 that optimizes online data research and analysis. It enables real-time access to online data providers.
i2 Chart Reader 6	6	i2	Charts Reader
i2 Chart Reader 7	7.0.7	i2	Charts Reader
i2 Image Files	6	i2	Image Editors
i2 Visual Notebook	6	i2	Visualization software, streamlines investigations
i2 Spelling Checker	6	i2	Image Editors
IIS URL Scan Tool	2.0		
IME Pass Client			
IME WWF Client			
JAVA™ 6 Update	1.6.0.60	Sun Micro	Program language compiler and environment
Live Update 3.2	3.2.0.68	Symantec	Software Update Tool
Microsoft .NET Framework 3.0 SP1	3.1.21022	Microsoft	Environment for building, deploying, and running web services and other applications
Microsoft .NET Framework 2.0 SP1	2.121022	Microsoft	Environment for building, deploying, and running web services and other applications
Microsoft .NET Framework 1.1	1.1.4322	Microsoft	Environment for building, deploying, and running web services and other applications
Microsoft Compressive Client1.0 for Window XP	1.0	Microsoft	
Microsoft Office Professional Plus Edition 2007	12.0.6215.1000	Microsoft	Electronic office tools
Microsoft Office 2003 Web components	11.0.6558.0	Microsoft	Allows embedding and linking to documents

BAL Software	Version	Vendor	Function/Component
Microsoft Office XP Web components	10.0.6619.0	Microsoft	Allows embedding and linking to documents
Mozilla Firefox	3.0.5	Mozilla	Web Browser
MS SQL Server 2005	9.2.3042.00	Microsoft	Database
MS SQL Server 2005 Backward Compatibility	8.05.2004	Microsoft	Database
MS SQL Server 2005 Books On-Line (English)	9.00.1399.06	Microsoft	Database
MS SQL Server Native Client	9.00.3042.00	Microsoft	Database
MS SQL Server Setup Support Files	9.00.4035.00	Microsoft	Database
MS SQL Server VSS Writer	9.00.4035.00	Microsoft	Database
MS User Mode Driver Framework Feature Pack 1.0	1.0	Microsoft	Build #5716
MSXML 6.0 Parser	6.10.1129.0	Microsoft	Text parser
MSXML 4 SP2	4.20.9818.0	Microsoft	Text parser
MSXML 4 SP2	4.20.9870.0	Microsoft	Text parser
MSXML 4 SP2	4.20.9848.0	Microsoft	Text parser
02 Micro Smartcard Driver	2.26.0000	02 Micro Electronics, Inc.	
OZ776 SCR CardBus	1.1.4.2	02 Micro Electronics, Inc.	
Psi	.12	GNU	Collaboration Tool
Python	2.4.1	Open Source	Object Oriented programming language
QuickTime	7.64.17.73	Apple	Audio and video file player
Query Tree MFWS Plugin	1.3.8	I2WD	MFWS Plugin
Roxio Activation Module	1.0	Roxio	Digital Media Software
Roxio Creator Audio	3.5.0	Roxio	Digital Media Software

BAL Software	Version	Vendor	Function/Component
Roxio Creator Copy	3.5.0	Roxio	Digital Media Software
Roxio Creator Data	3.5.0	Roxio	Digital Media Software
Roxio Creator DE	3.5.0	Roxio	Digital Media Software
Roxio Creator Tools	3.5.0	Roxio	Digital Media Software
Roxio Drag-to-Disc	9.1	Roxio	Digital Media Software
Roxio Express Labeler 3	3.2.1	Roxio	Digital Media Software
Roxio Update Manager	6.0.0	Roxio	Digital Media Software
Shared Add-in Extensibility update for MS.Net Framework 2.0	1.0.0	Microsoft	
Shared Add-in Support Update for MS.Net Framework 2.0	1.0.0	Microsoft	
Sigma Tel Audio	5.10.5210.0	SigmaTel	Digital audio processing
Smart Link 56k Voice modem			Voice modem
Sonic Cine Player Decoder Pack	4.2.0	Sonic Solutions	
Symantec AntiVirus	10.1.8000.8	Symantec	Virus detection
SQLXML 4	9.00.4035.00	Microsoft	
Synaptics Pointing Device	7.13.2.0	Synaptics	Pointing device
Threat Mapper 1.1 for ArcGIS Desktop	1.1		
Windows Internet Explorer 7 - 20070813.185237	7.0.5730.13	Microsoft	Web Browser
Windows Media Player 11	11.0	Microsoft	Media Player CD, DVD, streaming audio & video
Windows Media Format 11 Runtime	11.0	Microsoft	Media Player
Windows XP SP3	2008.0414.03 1535	Microsoft	
WinZip	10.0 (6685)	Winzip Computing LP	File compression
Xalan - Endorsed	1.00.0000	Overwatch	XML processing package

3.4 Possible Problems and Known Errors

See ReadMe document for DCGS-A V3.1.0P3 Multi-Function Work Station (MFWS) and Interoperability (IOP) Server, dated 17 February 2009, I2WD SIL.

3.5 Adaptation data

Not applicable

3.6 Related Documents

3.6.1 Post Clone Procedures

Refer FSE Training Guide in Section 2, Referenced Documents

3.6.2 Installation Procedures

DCGS-A V3.1.0P3 Multi-Function Work Station (MFWS) and Interoperability (IOP) Server ReadMe.doc, dated 17 February 2009, I2WD SIL

DCGS-A V3.1P3, Update Image Restore ReadMe.doc, dated 1 October 2009, I2WD SIL

3.6.3 Technical Bulletins

TB-DCGS 09-10087 – re: Workstation vulnerabilities fixes, 17 February 2009

TB-DCGS 09-10097 – re: DISA Gold/POA&M data, 17 February 2009

NOTE: TB-DCGS 09-10087 and TB-DCGS 09-10097 were implemented in the software baseline delivered to CTSF on 17 February 2009, and are under Application 2 server.

The following Technical Bulletins applies to the V3.1P3 SW baseline after 17 February 2009 delivery to CTSF:

TB Number	Configuration Systems	Title/Topic	PM DCGS-A Approved
DCGS 09-10094	MDC	Undeployment of DIB brain Adapter and /or PW update to xpipeline account, also adds DIB and portal versioning	11-May-09
DCGS 09-10095	IOP	IOP office 2007	11-May-09
DCGS 09-10099	MSMQ service on BALs	Fixes problem sending USMTF and PASS messages from BAL in standalone mode (4 March 2009)	14-May-09
DCGS 09-10100	APP1	Fixes APP1 homepage / baseline map problems (6 March 2009)	11-May-09
DCGS 09-10101	APP1	Fixes publishing Graphics to DIB problem (4 March 2009)	11-May-09
DCGS 09-10104	BAL	Adds Ft Hood Maps to BAL (23 March 2009)	7-May-09
DCGS 09-10106	BAL	Fixes problem with SWB1 IWEDA Client (31 March 2009)	11-May-09
DCGS 09-10107A	BAL & IOP	QT plugin ver1 3 8 1 update - allows working with BOTH OIF and OEF data (09 April 2009)	12-May-09
DCGS 09-10108	MDC	Adds Ft Huachuca Mini brain link to MDC portal (17 April 2009)	11-May-09
DCGS 09-10111	IOP	Fixes problem clearing the TED DB after a training event (20 April 2009)	7-May-09
DCGS 09-10112A	APP1, APP2, MDC, IOP, BAL	Configuration Assistant Update to v1 3 0 (5 May 09)	14-May-09
DCGS 09-10113	APP1	NAI fix for Firefox	11-May-09

TB Number	Configuration Systems	Title/Topic	PM DCGS-A Approved
DCGS 09-10115A	BAL	Fix for sending TED entities to Google Earth	18-May-09
DCGS 09-10116	BAL	Changing permission settings for DCGS-A User folder	7-May-09
DCGS 09-10120	MFWS	Allow the operator to enter a full non-western name in QuickForms and/or the Properties plugin without incorrectly mapping them to middle and last name fields	28-May-09
DCGS 09-10122	IOP, BAL	Applies to all v3 1 P3 DCGS-A DCGS IOP servers and BALs systems. It edits registry values to allow for the workflow between Google Earth and MFWS to be successful	3-Jun-09
DCGS 09-10123	BAL	Provides corrections to the DIB plug-in of the BAL MFWS. The TB corrects issues with the DIB usage found in the SIL Bug Tracker	15-Jun-09
DCGS 09-10126	IOP, BAL	Server Vulnerability Fixes. Hides DIB & Query Tree data drivers from the users display within Google Earth	3-Aug-09
DCGS 09-10128	APP2	Server Vulnerability Fixes. Users are unable to convert ANB7 charts to ANB6 charts	
DCGS 09-10129		Python 2.4 win32 extensions install	3-Aug-09
DCGS 09-10131B	MSG, SDE	Server Vulnerability Fixes (LISTA 0 7 5) for P3 & P5 systems (Red Hat 5 / 32 BIT)	21-Aug-09
DCGS 09-10132	BAL	Add mlRC chat to BAL baseline	24-Aug-09
DCGS 09-10133	BAL	Add correct ESRI Arc Desktop 9.2 License to Baseline for use of Tracking Analyst	2-Sep-09
DCGS 09-10134	BAL	Firefox Flash installation	2-Sep-09
DCGS 09-10137A	APP1	JBOSS windows service fix	10-Sep-09
DCGS 09-10147	APP1, APP2, MDC, IOP, BAL	Microsoft Windows Server / Workstation Vulnerability Fixes - SAT v1.2.1b	23-Sep-09
DCGS 09-10148	BAL, IOP	MFWS Merge Relationships, Deleted Entity Manager Updates	9-Oct-09
DCGS 09-10149A	MDC	JBOSS windows service fix (startDIBoss.cmd / wrapper.dll)	27-Oct-09
DCGS 09-10152	BAL, IOP	Removal of duplicate IIS Web folders from C:\DCGS directory	16-Oct-09
DCGS 09-10153	BAL, IOP	Issues Discovered in OIF and OEF_17 Feb 09 Image	23-Oct-09
DCGS 09-10155	MSG, SDE	Server Vulnerability Fixes - LISTA v0.7.7 (RHEL5 / 32 BIT) i386	27-Oct-09
DCGS 09-10157	APP1, APP2, IOP, MDC, BAL	Microsoft Windows Server / Workstation Vulnerability Fixes - SAT v1.2.1	3-Nov-09
DCGS 09-10159	BAL, IOP	Issues discovered in OIF and OEF (OW_P7) This TB supersedes TB 10153	6-Nov-09

3.6.4 *Overwatch MFWS Release 6.2*

DCGS-A V3.1, MFWS release 6.2, Document number: 102168, dated 15 January 2009, Overwatch
Textron Systems

3.7 COTS Software Sites

- 3D analyst (ArcGlobe)
 - <http://www.esri.com/software/arcgis/extensions/3danalyst/index.html>
- Acrobat Reader
 - <http://www.adobe.com>
 - <http://www.esri.com>
- Analyst Notebook
 - <http://www.i2.co.uk>
- Java
 - <http://java.sun.com/>
- Microsoft
 - <http://www.microsoft.com/>
- Netscape
 - <http://www.netscape.com/>
- Roxio
 - <http://roxio.com>
- Symantec
 - <http://www.symantec.com/index.htm>
- Winzip
 - <http://www.winzip.com/>
- WS_FTP
 - <http://www.ipswitch.com/>

3.8 Hardware Description

The following is a list of DCGS-A V3.1 P3 BALS hardware information:

Component	Description
Alienware Laptop - Model A51M	3.8 GHz, 2GB RAM memory, 17" display with high resolution graphics.
Dell Laptop - Model M90	2.33 GHz Intel Dual Processor Core, 3.25GB RAM memory, 93.1 GB hard drive, with NVIDIA graphics card, DCD-RW Optical Drive, Network Interface Card and a 17 inch display with high resolution graphics.
Laptop - Model Dell M6300	2.5 GHz Intel Core 2 Duo T9300, 4GB DDR2-667 SDRAM (2 DIMM), NVIDIA Quadro FX3600M 512 MB, 160 GB 7200RPM Hard Drive, Std Touchpad, 8x DVD+- & Roxio Creator , and a 17" wide screen WUXGA LCD.
Dell Precision 490 Workstation	1st Processor: Intel XEON DUAL CORE Processor 3.00GHZ, 2MB L2 Cache; 2nd Processor: Intel XEON DUAL CORE Processor 2.80GHZ, 2MB L2 Cache; 4GB, DDR2 ECC SDRAM Memory, 400MHZ; NVIDIA FX 4500 512MB 2 DUI OR GA 1st Hard Drive: 80GB Serial ATA 7200RPM Hard Drive w/Databurst Cache, Non-Raid, Precision 470/670; 2nd Hard Drive: 80GB Serial ATA 7200RPM Hard Drive with Databurst Cache Raid; Floppy Drive: 3.5, 1.44MB; 48X/32X CD-RW/DVD

Component	Description
	Combo.
Dell Precision T5400 Desk Top	1st Processor: Quad Core Xeon Proc X5450, 3.00GHz, 2X 6MB L2 Cache,1333MHz; 2nd Processor: Quad Core Xeon Proc X5450, 3.00GHz, 2X6MB L2 Cache,1333MHz, 4GB, DDR2 ECC SDRAM Memory 667MHz, 4X1GB; NVIDIA Quadro FX3700 512MB dual DVI Graphics Card; 160GB SATA, 10K RPM Hard Drive with 16MB DataBurst Cache; CD-ROM or DVD-ROM Drive: 16X DVD+/-RW.

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, xxx-xx- [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,
Fort Myer, VA 22211

**DEFENSE REQUEST FOR
SEARCH TERMS OF
RELEVANT COMPUTERS**

DATED: 30 March 2012

1. The Defense, in consultation with its computer forensic experts, requests the following additional search terms¹:

- a) M-IRC Chat²
- b) Wget
- c) Internet Download Manager
- d) Virtual DJ
- e) Free YouTube Downloader
- f) VLC Media Player
- g) UMLayer
- h) UTorrent
- i) IrfanView
- j) Paint.NET
- k) GEOTRANS
- l) Grid Extractor
- m) Google Earth
- n) Picasa
- o) XnView
- p) GIMP
- q) ubuntu
- r) Skype
- s) Any-Video-Converter
- t) RoboForm

¹ The Defense incorporate the Court's Order to search for Wget, M-IRC Chat, Google Earth, movies, games, and music. By submitting this list, the Defense does not waive its request for a more detailed search as referenced in the Defense Renewal of Motion to Compel Discovery of Computers also dated 30 March 2012. The Defense also does not concede that this limited search complies with either R.C.M. 701(a)(2) or R.C.M. 701(a)(6).

² The Defense requests that the Government provide the software version of each identified program. For instance, M-IRC Chat, if there are multiple versions of this single program on the various computers, the Defense requests that the Government list each version found. A specific version of software may have been authorized on the DCGS-A, while newer versions were not. Thus, the Defense needs the exact version found during the Government's review.

- u) BitTorrent
- v) Applian FLV Media Player
- w) Yahoo Messenger
- x) Windows Live Messenger
- y) ALMP
- z) Pidgin
- aa) Digsby
- bb) Thunderbird
- cc) iTunes
- dd) Songbird
- ee) Spotify
- ff) Winamp
- gg) Google Talk
- hh) RealPlayer
- ii) Media Player Classic
- jj) Foxit Reader

2. The point of contact for this memorandum is the undersigned at (401) 744-3007 or by e-mail at coombs@armycourt martialdefense.com.

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

UNITED STATES OF AMERICA)

v.)

Prosecution Notification
to the Court

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

20 April 2012

The United States responds to the Court's Order, dated 23 March 2012 as follows:

1. **Hard Drive Searches.** The Computer Crimes Investigative Unit (CCIU) conducted a review pursuant to the Court's order. Based on input from the government security expert, the United States could not determine the classification of 460 filenames in Attachment 4 because they were written in Arabic; therefore, this information has been redacted from the attachment.¹ Below is a summary of their findings and attached are the Agent's Investigation Reports:

a. Of the fourteen hard drives, only four were found to contain valid file systems, the remaining drives were blank, contained no accessible data, or were inoperable.

b. The VLC application was installed on Items 1 and 11.

c. The M-IRC application was installed in several locations on Items 1 and 11.

d. The Media Player Classic application was installed on Item 11.

e. Audio and video files of apparent entertainment values were identified on the examined images.

2. The prosecution contacted the DOS, FBI, CIA, DIA, and ONCIX to determine whether these agencies contain any forensic results or investigative files relevant to this case.²

(1) **DOS.** DOS has forensic results and investigative files. The United States reviewed this information for evidence that is favorable to the accused and material to either guilt or punishment. Additionally, prior to the Court's order, the United States produced this information to the defense.

(2) **FBI.** FBI has forensic results and investigative files. The United States is reviewing this information for evidence that is favorable to the accused and material to either guilt or

¹ The United States is diligently working to determine who can provide translation of these Arabic names.

² On 16 April 2012, the Court granted the Government's motion for leave of the Court to extend the time to respond from 20 April 2012 to 2 May 2012 as to whether the CIA will release classified information in original form, provide for limited disclosure under MRE 505(g)(2), or invoke the classified information privilege under MRE 505(c).

punishment. Additionally, prior to the Court's order, the United States started producing this information to the defense.

(3) **DIA.** DIA does not have any forensic results or investigative files.

(4) **ONCIX.** ONCIX does not have any forensic results or investigative files.

3. At this time, the United States anticipates that the **FBI** is the only government entity that is a custodian of classified forensic results or investigative files relevant to this case that will seek limited disclosure IAW MRE 505(g)(2).

A handwritten signature in black ink, consisting of a large, stylized loop followed by a horizontal line and a short vertical stroke.

ASHDEN FEIN
MAJ, JA
Trial Counsel

Appellate Exhibit 56
Attachments
252 pages
ordered sealed for Reason 6
Military Judge's Seal Order
dated 20 August 2013
stored in the original Record
of Trial

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army, xxx-xx-)

Headquarters and Headquarters Company, U.S.)

Army Garrison, Joint Base Myer-Henderson Hall,)
Fort Myer, VA 22211)

**DEFENSE MOTION TO DISMISS
BASED UPON UNREASONABLE
MULTIPLICATION OF
CHARGES**

DATED: 29 March 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by counsel, pursuant to applicable case law, requests this Court to dismiss and/or consolidate several specifications because, as charged by the Government, they constitute an unreasonable multiplication of charges. The Defense submits that the Government has unreasonably multiplied the charges against PFC Manning by charging violations of multiple provisions of Title 18 of the United States Code for conduct that should only be charged, if at all, as a violation of one provision of Title 18. Additionally, the Government has unreasonably multiplied the charges against PFC Manning by breaking down single transactions into multiple specifications each.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. The Defense, as the moving party, bears the burden of this motion by a preponderance of the evidence pursuant to R.C.M. 905(c)(1) and (2).

FACTS

3. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of conduct prejudicial to good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting government property, and two specifications of knowingly exceeding authorized access to a government computer, in violation of Articles 92, 104, and 134, Uniform Code of Military Justice (UCMJ) 10 U.S.C. §§ 892, 904, 934 (2010). The case has been referred to a general court martial by the convening authority with a special instruction that the case is not a capital referral.

4. In Specification 4 of Charge II, PFC Manning is alleged to have, "at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 5

January 2010," stolen, purloined, or knowingly converted "the Combined Information Data Network Exchange Iraq database containing more than 380,000 records belonging to the United States Government," in violation of 18 U.S.C. Section 641 and Article 134. In Specification 5 of the same charge, it is alleged that PFC Manning, having unauthorized possession of classified Combined Information Data Network Exchange Iraq database records, did, at the same place specified in Specification 4 between on or about 31 December 2009 and on or about 9 February 2010, willfully communicate, deliver, transmit, or cause to be communicated, delivered or transmitted, these records to a person not entitled to receive them with reason to believe that the records could be used to the injury of the United States or to the advantage of any foreign nation, in violation of 18 U.S.C. Section 793(e) and Article 134.

5. In Specification 6 of Charge II, PFC Manning is alleged to have, "at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 8 January 2010," stolen, purloined, or knowingly converted "the Combined Information Data Network Exchange Afghanistan database containing more than 90,000 records belonging to the United States Government," in violation of Section 641 and Article 134. Additionally, in Specification 7 of the same charge, it is alleged that PFC Manning, having unauthorized possession of classified records contained on the Combined Information Data Network Exchange Afghanistan database, did, at the same place specified in Specification 6 between on or about 31 December 2009 and on or about 9 February 2010, willfully communicate, deliver, transmit, or cause to be communicated, delivered or transmitted, these records to a person not entitled to receive them with reason to believe that the records could be used to the injury of the United States or to the advantage of any foreign nation, in violation of Section 793(e) and Article 134.

6. In Specification 8 of Charge II, PFC Manning is alleged to have, "at or near Contingency Operating Station Hammer, Iraq, on or about 8 March 2010," stolen, purloined, or knowingly converted "a United States Southern Command database containing more than 700 records belonging to the United States Government," in violation of Section 641 and Article 134. Specification 9 of the same charge alleges that PFC Manning, having unauthorized possession of classified records contained on the database specified in Specification 8, did, at the same place specified in Specification 8 between on or about 8 March 2010 and on or about 27 May 2010, willfully communicate, deliver, transmit, or cause to be communicated, delivered or transmitted, these records to a person not entitled to receive them with reason to believe that the records could be used to the injury of the United States or to the advantage of any foreign nation, in violation of Section 793(e) and Article 134.

7. In Specification 12 of Charge II, PFC Manning is alleged to have, "at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 4 May 2010," stolen, purloined, or knowingly converted "the Department of State Net-Centric Diplomacy database containing more than 250,000 records belonging to the United States Government," in violation of Section 641 and Article 134. Specification 13 of the same charge alleges that PFC Manning, at the same place specified in Specification 12 between on or about 28 March 2010 and on or about 27 May 2010, knowingly exceeded his authorized access on a Secret Internet Protocol Router computer, obtained classified Department of State cables determined to require protection against unauthorized disclosure, and willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, these cables to a

person not entitled to receive them with reason to believe that these cables so obtained could be used to the injury of the United States, in violation of 18 U.S.C. Section 1030(a)(1) and Article 134.

8. In Specification 10 of Charge II, it is alleged that PFC Manning, having unauthorized possession of classified records relating to a military operation in Farah Province, Afghanistan occurring on or about 4 May 2009, did, "at or near Contingency Operating Station Hammer, Iraq, between on or about 11 April 2010 and on or about 27 May 2010," willfully communicate, deliver, transmit, or cause to be communicated, delivered or transmitted, these records to a person not entitled to receive them with reason to believe that the records could be used to the injury of the United States or to the advantage of any foreign nation, in violation of Section 793(e) and Article 134.

9. In Specification 11 of Charge II, it is alleged that PFC Manning, having unauthorized possession of a file containing a video relating to the national defense, did, "at or near Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 8 January 2010," willfully communicate, deliver, transmit, or cause to be communicated, delivered or transmitted, this file to a person not entitled to receive it with reason to believe that the file could be used to the injury of the United States or to the advantage of any foreign nation, in violation of Section 793(e) and Article 134.

WITNESSES/EVIDENCE

10. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this Court to consider the following evidence in support of the Defense's motion.

- a. Charge Sheet;
- b. Continuation of DD Form 457;
- c. SD Card Forensic Report, Bates # 00125319-31, at 1-2, 9 (provided as a classified enclosure by the Government);
- d. PFC Manning's Primary SIPRNET Computer Forensic Report, Bates # 00211037-110, at 51-52 (provided as a classified enclosure by the Government);
- e. PFC Manning's Personal Computer Forensic Report, Bates # 00124283-362, at 49, 54-58, 65-68. (provided as a classified enclosure by the Government).

LEGAL AUTHORITY AND ARGUMENT

11. The Manual for Courts-Martial (MCM) directs that "[w]hat is substantially one transaction should not be made the basis for an unreasonable multiplication of charges against one person."

Rule for Court-Martial 307(c)(4). “[T]he prohibition against unreasonable multiplication of charges addresses those features of military law that increase the potential for overreaching in the exercise of prosecutorial discretion.” *United States v. Quiroz*, 55 M.J. 334, 337 (C.A.A.F. 2001).

12. The Court of Appeals for the Armed Forces has set forth a five factor test for assessing claims of unreasonable multiplication of charges:

- (1) Did the accused object at trial that there was an unreasonable multiplication of charges and/or specifications?
- (2) Is each charge and specification aimed at distinctly separate criminal acts?
- (3) Does the number of charges and specifications misrepresent or exaggerate the [accused's] criminality?
- (4) Does the number of charges and specifications unreasonably increase the [accused's] punitive exposure?
- (5) Is there any evidence of prosecutorial overreaching or abuse in the drafting of the charges?

United States v. Pauling, 60 M.J. 91, 95 (C.A.A.F. 2004); see *Quiroz*, 55 M.J. at 338-39 (articulating these five factors). The Court has further instructed that “[t]hese factors must be balanced, with no single factor necessarily governing the result.” *Pauling*, 60 M.J. at 95. Where a trial court finds an unreasonable multiplication of charges, dismissal of the unreasonably multiplied charges is an available remedy. *United States v. Roderick*, 62 M.J. 425, 433 (C.A.A.F. 2006). Consolidation of the unreasonably multiplied charges is also a remedy available to the trial court. *United States v. Gilchrist*, 61 M.J. 785, 789 (A. Ct. Crim. App. 2005). In any event, once an unreasonable multiplication of charges is shown, “it [is] incumbent on the trial judge . . . either to consolidate the specifications or to dismiss a specification[.]” *United States v. Burris*, 21 M.J. 82, 82 (C.M.A. 1985).

13. When analyzed under this five factor test, the Government’s drafting of several specifications in the instant case has run afoul of the prohibition against unreasonable multiplication of charges. First, multiple specifications of Charge II allege violations of either Section 641 or Section 793(e). In several such instances, the same transaction has been split into a Section 641 specification and a Section 793(e) specification. This creative drafting by the Government drastically exaggerates PFC Manning’s criminality and unreasonably increases his punitive exposure. Second, Specifications 12 and 13 of Charge II charge violations of Sections 641 and 1030(a)(1), respectively. However, the alleged conduct behind these two charged offenses constitutes only one transaction. By splitting this conduct into two separate offenses, the Government has again unreasonably multiplied the charges against PFC Manning. Finally, several different specifications of Charge II allege violations of either Sections 641, 793(e), or 1030(a)(1). Yet the alleged conduct behind several of these specifications occurred in the same transaction on the same day. The Government has again sought to exaggerate PFC Manning’s criminality and increase his punitive exposure by creatively separating one transaction into

multiple specifications. Each instance of unreasonable multiplication of charges is discussed in turn.

A. The Government Unreasonably Multiplied the Charges Against PFC Manning by Repeatedly Splitting the Same Transaction Into One Specification Alleging a Violation of Section 641 and One Specification Alleging a Violation of Section 793(e)

14. The Defense submits that the Government unreasonably multiplied the charges against PFC Manning by splitting one transaction into two specifications: one alleging a violation of Section 641 and one alleging a violation of Section 793(e). The conduct underlying a particular Section 641 violation cannot be logically separated from the conduct underlying the corresponding Section 793(e) violation. In maintaining this artificial distinction in these specifications, the Government has exaggerated PFC Manning's criminality and unreasonably increased his punitive exposure. Moreover, the Government has unreasonably multiplied charges against PFC Manning in this manner three separate times in Charge II.

15. Specifications 4 and 5 of Charge II allege that PFC Manning violated Sections 641 and 793(e), respectively, when he stole, purloined, or knowingly converted the Combined Information Data Network Exchange Iraq database and then disclosed certain classified records on that database to a person not entitled to receive those records. These specifications deal with the same transaction – PFC Manning's alleged unauthorized possession and disclosure of the Combined Information Data Network Exchange Iraq database records.

16. Additionally, Specifications 6 and 7 of Charge II allege that PFC Manning violated Sections 641 and 793(e), respectively, when he stole, purloined or knowingly converted the Combined Information Data Network Exchange Afghanistan database and then impermissibly disclosed certain classified records on that database. Like Specifications 4 and 5, Specifications 6 and 7 of Charge II deal with the same transaction – PFC Manning's alleged unauthorized possession and disclosure of the Combined Information Data Network Exchange Afghanistan database records.

17. Finally, Specifications 8 and 9 of Charge II allege that PFC Manning violated Sections 641 and 793(e), respectively, when he stole, purloined or knowingly converted a United States Southern Command database and then impermissibly disclosed certain classified records on that database. These specifications also attempt to target one transaction – the alleged unauthorized possession and disclosure of the records on a United States Southern Command database.

18. Application of the five factor test for unreasonable multiplication of charges demonstrates that the Government has unreasonably multiplied the charges against PFC Manning by drafting these specifications:

a. First, this motion serves as PFC Manning's objection to the unreasonable multiplication of charges, so this factor must be resolved in his favor. *See United States v. Paxton*, 64 M.J. 484, 491 (C.A.A.F. 2007).

b. Second, these specifications are not directed at distinctly separate acts. See *Quiroz*, 55 M.J. at 338. Taking Specifications 4 and 5 as an example, the alleged conduct behind these two specifications cannot logically be separated in the manner the Government has attempted. Before PFC Manning could have secured unauthorized possession of the relevant database records and before he could disclose these records, see 18 U.S.C. § 793(e), he first needed to secure possession of these records. In order to secure possession of these materials, PFC Manning, according to the Government, stole, purloined, or knowingly converted the database on which these materials were stored. Therefore, under the Government's theory, PFC Manning could not gain unauthorized possession of the records he allegedly disclosed without first stealing, purloining, or knowingly converting the database. The Section 641 violation charged in Specification 4 was simply the first step in the transaction that was the alleged Section 793(e) violation charged in Specification 5; without the theft or conversion of the database, there could be no unauthorized possession of the records. The Navy-Marine Court of Military Review's decision in *United States v. Johnson* is instructive. In *Johnson*, the accused failed to inform the Personal Support Detachment that he was no longer entitled to receive Basic Allowance for Quarters (BAQ) and Variable Housing Allowance (VHA). 39 M.J. 707, 708-10 (N.M.C.M.R. 1993). He continued to receive BAQ and VHA to which he was not entitled for eight months. *Id.* at 711. The Government elected to charge the accused with eight specifications of larceny of BAQ and VHA, one specification for each month of the accused's improper receipt of BAQ and VHA. *Id.* On appeal, the accused argued that this represented an unreasonable multiplication of charges. *Id.* The court agreed, explaining that "[w]hat happened here was essentially a single course of theft of Government funds over an extended period and not eight thefts. Therefore, the eight specifications shall be merged into one." *Id.*; see also *Burris*, 21 M.J. at 82 (finding an unreasonable multiplication of charges where "substantially one transaction" – the accused's false statements on two forms in his application for base housing – was charged as two separate specifications). Similarly, Specifications 4 and 5 in the instant case are not directed at distinctly separate acts. Rather, like the eight specifications in *Johnson* that were directed at a single course of theft, see 39 M.J. at 711, Specifications 4 and 5 are directed at a single course of alleged conduct. The same can be said for Specifications 6 and 7 of Charge II and for Specifications 8 and 9 of Charge II. Therefore, the second factor must also be resolved in PFC Manning's favor.

c. Third, the number of specifications misrepresent and exaggerate PFC Manning's criminality. See *Quiroz*, 55 M.J. at 338. One transaction – the Section 793(e) violation requiring unauthorized possession and disclosure of classified records – has been made the subject of two specifications through the Government's expansive charging in Specifications 4 and 5. The Government has repeated this duplication effort with respect to Specifications 6 and 7 and with respect to Specifications 8 and 9. Moreover, there are numerous other instances where the Government has similarly separated other transactions into two separate specifications in Charge II. See Argument, Parts B & C, *infra*.

d. Fourth, this overcharging unreasonably increases PFC Manning's punitive exposure. See *Quiroz*, 55 M.J. at 338-39. Congress has provided that the maximum punishment for a violation of Section 793(e) is imprisonment for ten years. 18 U.S.C. § 793(e). Similarly, the maximum punishment for a violation of Section 641 is also ten years. *Id.* § 641. Congress could have cross referenced Sections 641 and 793(e), but it chose not to do so. If the Government is permitted to

maintain both Specifications 4 and 5, the maximum punishment for one transaction – an unauthorized possession and disclosure under Section 793(e) – would become twenty years instead of the ten years that Congress chose. Doubling the punitive exposure for one transaction is plainly unreasonable. See *United States v. Quiroz*, 57 M.J. 583, 586 (N-M. Ct. Crim. App. 2002), *on remand from*, 55 M.J. 334 (C.A.A.F. 2001). Indeed, the Navy-Marine Court of Criminal Appeals confronted a similar doubling of the punitive exposure of an accused in *Quiroz*:

By charging [Quiroz] twice for the sale of the same C-4, the prosecution magnified the extent of his criminal activity and increased the maximum permissible confinement for this sale from 10 years to 20 years The doubling of [Quiroz's] punitive exposure by 10 years is a significant increase that does not appear to be warranted by anything in the record. We, therefore, find that the charges in question did unreasonably increase [Quiroz's] punitive exposure.

Id. Here, as in *Quiroz*, the Government is attempting to double PFC Manning's punitive exposure by artificially splitting one act into two offenses. Additionally, the United States Supreme Court has instructed that the concept of "punishment" encompasses not only the imposition of sentence, but the actual conviction as well. *Ball v. United States*, 470 U.S. 856, 861, 864-65 (1985). Therefore, if the Government's expansive charging is permitted, PFC Manning could be subjected to twice as many convictions and twice as much punishment for what is substantially one Section 793(e) violation. The same can be said for the Government's drafting of Specifications 6 and 7 and Specifications 8 and 9.

e. Finally, there is evidence of prosecutorial overreaching and abuse in the drafting of the specifications. Charge II itself demonstrates the existence of prosecutorial overreaching. The Government has on three occasions sought to separate one transaction – a violation of Section 793(e) by unauthorized possession and disclosure of classified information – into two offenses. Moreover, the Government has similarly broken down other transactions into their component parts as well. See Argument, Parts B & C, *infra*. The reason for this unnatural breakdown of these transactions is obvious: the division serves no purpose other than to pile on the charges against PFC Manning in order to increase the likelihood of a severe sentence if he is convicted. This is precisely the type of overreaching that the prohibition against unreasonable multiplication of charges is intended to guard against. See *Quiroz*, 55 M.J. at 337. Additionally, in Specifications 4, 6, and 8 of Charge II, the Government has pushed Section 641 to the edge of its permissible application. Congress has legislated comprehensively in the field of information relating to the national defense. It has enacted Section 793(e), which punishes whoever, having unauthorized possession of information relating to the national defense, willfully discloses that information with reason to believe that the information could be used to the injury of the United States or to the advantage of a foreign nation. 18 U.S.C. § 793(e). It has also enacted Section 1030(a)(1), which punishes whoever exceeds authorized access to a computer, obtains covered information relating to the national defense or foreign relations, and willfully discloses that information with reason to believe that the information could be used to the injury of the United States or to the advantage of any foreign nation. *Id.* § 1030(a)(1). Some judges have expressed doubts over whether Section 641 can even be applied to information relating to the national defense without seriously disrupting this comprehensive framework established by Congress.

See *United States v. Truong Dinh Hung*, 629 F.2d 908, 926 (4th Cir. 1980) (opinion of Winter, J.) (“If [Section] 641 were extended to penalize the unauthorized disclosure of classified information, it would greatly alter this meticulously woven fabric of criminal sanctions.”); *id.* at 928 (“[B]ecause a criminal prohibition against the unauthorized disclosure of classified information would be inconsistent with the existing pattern of criminal statutes governing the disclosure of classified information and because Congress has always refused to enact a statute like [Section] 641 applicable to the disclosure of classified information . . . [Section] 641 cannot be interpreted to punish the unauthorized disclosure of classified information.”); see also *United States v. Jeter*, 775 F.2d 670, 682 (6th Cir. 1985) (“We do not attempt to determine the constitutionality of Section 641 in a ‘Pentagon Papers’ type of situation.”). The fact that the Government in this case has elected to use Section 641 in this gray area to increase the charges against PFC Manning for what is really only an alleged Section 793(e) violation is further evidence of prosecutorial overreaching and abuse in the drafting of these specifications.

19. Therefore, this Court should determine that: Specifications 4 and 5 of Charge II constitute an unreasonable multiplication of charges; Specifications 6 and 7 of Charge II constitute an unreasonable multiplication of charges; and Specifications 8 and 9 of Charge II constitute an unreasonable multiplication of charges. Accordingly this Court should dismiss Specifications 4, 6, and 8 of Charge II.

B. The Government Unreasonably Multiplied the Charges Against PFC Manning by Splitting the Same Transaction into One Specification Alleging a Violation of Section 641 and One Specification Alleging a Violation of Section 1030(a)(1)

20. The Defense further submits that the Government again unreasonably multiplied the charges against PFC Manning by splitting one other alleged transaction into two separate specifications: one alleging a violation of Section 641 and one alleging a violation of Section 1030(a)(1). Specifications 12 and 13 of Charge II allege that PFC Manning violated Sections 641 and 1030(a)(1), respectively, when he stole, purloined, or knowingly converted the Department of State Net-Centric Diplomacy database and then disclosed certain classified records on that database to a person not entitled to receive those records. These specifications deal with the same transaction – PFC Manning’s alleged exceeding authorized access to obtain the Department of State Net-Centric Diplomacy database records and his subsequent disclosure of them. These specifications constitute an unreasonable multiplication of charges:

a. First, this motion serves as PFC Manning’s objection to the unreasonable multiplication of charges, so this factor must be resolved in his favor. See *Paxton*, 64 M.J. at 491.

b. Second, Specifications 12 and 13 are not directed at distinctly separate acts. See *Quiroz*, 55 M.J. at 338. The alleged conduct constituting PFC Manning’s Section 641 violation is identical to the first step in the charged Section 1030(a)(1) violation – exceeding authorized access and thereby obtaining covered information. Under the Government’s theory, before he could wilfully disclose information covered by Section 1030(a)(1), PFC Manning was first required to exceed authorized access to a computer and to obtain covered information. How did PFC Manning accomplish these necessary prerequisite steps? According to the Government, it

was by and through his theft or knowing conversion of the Department of State Net-Centric Diplomacy database. In other words, PFC Manning's alleged theft or conversion of the database was the alleged exceeding of his authorized access and the obtaining of covered information, all rolled into one. Therefore, far from targeting distinctly separated acts in Specifications 12 and 13, the Government has artificially broken down one act into two offenses. *See Burris*, 21 M.J. at 82; *Johnson*, 39 M.J. at 711.

c. Third, Specifications 12 and 13 misrepresent and exaggerate PFC Manning's criminality. *See Quiroz*, 55 M.J. at 338. One alleged transaction – the Section 1030(a)(1) violation requiring exceeding authorized access, obtaining of covered information, and disclosure of that information – has been made the subject of two specifications through the Government's expansive charging in Specifications 12 and 13. When this effort to exaggerate PFC Manning's criminality is coupled with the several other instances of unreasonable multiplication of charges, *see* Argument, Part A, *supra*, and Part C, *infra*, the effort to misrepresent and exaggerate his criminality is manifest.

d. Fourth, this overcharging unreasonably increases PFC Manning's punitive exposure. *See Quiroz*, 55 M.J. at 338-39. Congress has provided that the maximum punishment for a violation of Section 1030(a)(1), as charged by the Government in this case, is imprisonment for ten years. 18 U.S.C. § 1030(c)(1)(A). Similarly, the maximum punishment for a violation of Section 641 is also ten years. *Id.* § 641. Congress could have cross referenced Sections 641 and 1030 (a)(1), but it chose not to do so. If the Government is permitted to maintain both Specifications 12 and 13, the maximum punishment for one transaction – exceeding authorized access, obtaining covered information, and disclosing it in violation of Section 1030(a)(1) – would become twenty years instead of the ten years that Congress chose. Doubling the available maximum punishment in this manner is, for the reasons discussed by the Navy-Marine Court of Criminal Appeals in *Quiroz*, a textbook example of unreasonably increasing an accused's punitive exposure. *See Quiroz*, 57 M.J. at 586; *see also* Argument, Part A, *supra*. Moreover, the mere attempt to secure an extra conviction for this one transaction also increases PFC Manning's punitive exposure. *See Ball*, 470 U.S. at 861, 864-65.

e. Finally, there is evidence of prosecutorial overreaching and abuse in the way in which Specifications 12 and 13 have been drafted. This overreaching and abuse is plainly evident from the purpose and effect of charging one transaction – the alleged Section 1030(a)(1) violation – as two separate offenses. It is clear that both the purpose and effect of this artificial splitting of one offense into two is to pile on the charges against PFC Manning to exaggerate his criminality and increase his punitive exposure. Moreover, the Government has similarly broken down other single transactions into separate specifications. *See* Argument, Part A, *supra*, and Part C, *infra*. This is precisely the type of prosecutorial overreaching that the prohibition against unreasonable multiplication of charges is intended to guard against. *See Quiroz*, 55 M.J. at 337. Additionally, the prosecutorial overreaching and abuse is similarly evident from the Government's decision to charge a Section 641 violation for the use of a computer to obtain information covered by Section 1030(a)(1). As Professor Orin Kerr has observed, because Section 641 is such an awkward tool to combat misuse of a computer to obtain information on the computer, Congress passed Section 1030:

Because no res can be defined in the great majority of cases, [Section] 641 is an ill-suited tool to try to deter unauthorized use of federal government computer systems.

Conversion's inability to serve as a useful doctrinal tool to deter unauthorized computer use has led to a number of federal and state statutory measures to meet this important need. The Computer Fraud and Abuse Act [, 18 U.S.C. Section 1030,] punishes a broad range of computer crimes. These crimes include the unauthorized access and procurement of classified national defense data by computer[.]

Orin S. Kerr, Note, *The Limits of Computer Conversion*: United States v. Collins, 9 Harv. J.L. & Tech. 205, 211 (1996) (footnotes omitted). Therefore, just as the Government has pushed Section 641 to its limit by charging PFC Manning with Section 641 violations for his alleged Section 793(e) violations, *see* Argument Part A, *supra*, the Government has here elected to use Section 641, an ill-suited tool for deterring computer misuse, in conjunction with Section 1030(a)(1), a provision enacted to rectify the deficiencies of using Section 641 to combat computer misuse. *See* Kerr, *supra*, at 211. This redundancy in charging is no accident; it represents clear evidence that the Government has sought to charge PFC Manning with any violation that could, by stretching the imagination, fit his alleged conduct. The doctrine of unreasonable multiplication of charges prevents the Government from piling on in this manner any and all conceivable charges. *See Quiroz*, 55 M.J. at 337.

21. For these reasons, this Court should determine that Specifications 12 and 13 of Charge II constitute an unreasonable multiplication of charges and should accordingly dismiss Specification 12 of Charge II.

C. The Government Unreasonably Multiplied the Charges Against PFC Manning by Splitting the Same Transaction that Occurred on the Same Day into Multiple Specifications

22. The Defense submits that for several specifications the Government has unreasonably multiplied the charges against PFC Manning by splitting a single transaction that occurred on the same day into multiple specifications. The Government has done this on two occasions in Charge II. Each instance of unreasonable multiplication of charges is discussed in turn.

The Conduct Alleged in Specifications 4, 5, 6, and 7 of Charge II Constitutes a Single Transaction Committed on the Same Day

23. Specifications 4 and 5 of Charge II allege that PFC Manning violated Sections 641 and 793(e), respectively, when he stole, purloined, or knowingly converted the Combined Information Data Network Exchange Iraq database and then disclosed certain classified records on that database to a person not entitled to receive those records. Additionally, Specifications 6 and 7 of Charge II allege that PFC Manning violated Sections 641 and 793(e), respectively,

when he stole, purloined or knowingly converted the Combined Information Data Network Exchange Afghanistan database and then impermissibly disclosed certain classified records on that database. The conduct alleged in all four of these specifications occurred on the same day.¹

24. Additionally, the disclosures of the Combined Information Data Network Exchange Iraq database records and the Combined Information Data Network Exchange Afghanistan database records occurred at the same time. See footnote 1. Therefore, PFC Manning committed, at most, one Section 793(e) violation in disclosing these records. The Government, however, has attempted to charge this one violation as four violations – two Section 641 violations (Specifications 4 and 6) and two Section 793(e) violations (Specifications 5 and 7). This multiplication of charges is unreasonable:

a. First, this motion serves as PFC Manning's objection to the unreasonable multiplication of charges, so this factor must be resolved in his favor. See *Paxton*, 64 M.J. at 491.

b. Second, Specifications 4, 5, 6 and 7 are directed at the same conduct; they are not directed at distinctly separate acts. See *Quiroz*, 55 M.J. at 338. For reasons discussed above, the Section 641 violations alleged in Specifications 4 and 6 are unreasonable multiplications of the Section 793(e) violations alleged in Specifications 5 and 7, respectively. See Argument, Part A, *supra*. Additionally, the alleged disclosure of records from the Combined Information Data Network Exchange Iraq database targeted in Specification 5 and the alleged disclosure of records from the Combined Information Data Network Exchange Afghanistan database targeted in Specification 7 took place at the same time on the same day. In other words, there were not two disclosures, as Specifications 5 and 7 would lead one to believe, but only one disclosure of records from both databases. Therefore, the Government, in drafting Specifications 4, 5, 6 and 7, has taken the conduct behind a single disclosure and made it subject to four separate specifications. The Army Court of Criminal Appeals' decision in *Gilchrist* is instructive. In *Gilchrist*, the accused entered another's room and stole \$60.00 cash and some Xanax pills worth about \$20.00. 61 M.J. at 788. The Government charged the larceny of the cash as one specification and the larceny of the pills as another specification. *Id.* The *Gilchrist* Court unanimously found this to be an unreasonable multiplication of charges. *Id.* at 789. The court concluded that the larceny of the cash and the larceny of the pills were parts of a single larceny, and only a single larceny should have been charged. *Id.* The court quoted from the MCM as follows: "When a larceny of several articles is committed at substantially the same time and place, it is a single larceny even though the articles belong to different persons. Thus, if a thief . . . goes into a room and takes property belonging to various persons, there is but one larceny . . ." *Id.* (quoting MCM, Part IV, para. 46(c)(1)(h)(ii)) (ellipses in original). Elaborating on this point, the court explained that "specifications constitute an unreasonable multiplication of charges as a matter of policy when . . . what is substantially one transaction is unreasonably broken down into its component parts and charged separately." *Id.* at 789 n.5; see also *Burris*, 21 M.J. at 82; *United States v. Box*, 2009 WL 6865266, at *1 (A. Ct. Crim. App. Feb 27, 2009) (unpublished) (finding an unreasonable multiplication of charges where accused stole three items from a gym locker and Government drafted two specifications for this single theft); *United States v. Thomas*, 2008 WL 8084967, at *1 (A. Ct. Crim. App. April 30, 2008) (unpublished) (finding an unreasonable multiplication of charges where accused stole a laptop and a cell phone from the same victim and Government charged the larceny of the

¹ See SD Card Forensic Report, Bates # 00125319-31, at 1-2, 9.

laptop in one specification and the larceny of the cell phone in a separate specification); *cf. Johnson*, 39 M.J. at 711 (finding a single course of theft spanning eight months as opposed to eight separate thefts). In this case, the Government has run afoul of this prohibition in drafting Specifications 4, 5, 6, and 7 of Charge II. Just as the Government in *Gilchrist* impermissibly broke down a single larceny into two separate larcenies, *see* 61 M.J. at 788-89, the Government here has impermissibly broken down an alleged single disclosure of multiple records (i.e. a single violation of Section 793(e)) into two separate disclosures (i.e. two separate violations of Section 793(e)). Compounding this problem, the Government has further broken down each of these two alleged violations of Section 793(e) into two even smaller parts: one violation of Section 641 and one violation of Section 793(e). *See* Argument, Part A, *supra*. Thus, the Government in this case has broken down a single disclosure into four separate violations. *Gilchrist* plainly forbids such a balkanization of a single transaction. *See* 61 M.J. at 788-89.

c. Third, the breaking down of one transaction into four specifications in this manner misrepresents and exaggerates PFC Manning's criminality. *See Quiroz*, 55 M.J. at 338. A single disclosure has been made the subject of four specifications.

d. Fourth, this overcharging unreasonably increases PFC Manning's punitive exposure. *See Quiroz*, 55 M.J. at 338-39. Instead of facing a maximum ten year sentence for his alleged Section 793(e) violation (the single disclosure), PFC Manning faces four specifications, each containing a ten year maximum punishment. *See* 18 U.S.C. § 641 (containing maximum punishment of ten years imprisonment); *id.* § 793(e) (same). Thus, the Government has quadrupled PFC Manning's punitive exposure for this one alleged disclosure by creatively charging it as four specifications instead of one. If doubling an accused's punitive exposure is unreasonable, *see Quiroz*, 57 M.J. at 586, surely quadrupling an accused's punitive exposure is even more unreasonable.

e. Finally, the Government's decision to multiply a single disclosure into four specifications readily demonstrates prosecutorial overreaching and abuse. Both the purpose and effect of this artificial splitting of one offense into four is to unnecessarily pile on the charges against PFC Manning to exaggerate his criminality and increase his punitive exposure. Preventing this prosecutorial overreaching is the main concern of the principle of unreasonable multiplication of charges. *See Quiroz*, 55 M.J. at 337.

25. For these reasons, this Court should determine that Specifications 4, 5, 6, and 7 of Charge II constitute an unreasonable multiplication of charges. Accordingly, this Court should dismiss Specifications 4 and 6 of Charge II, *see* Argument Part A, *supra*, and should consolidate Specifications 5 and 7 of Charge II into a single specification.

The Conduct Alleged in Specifications 10 and 11 of Charge II Constitute a Single Transaction Committed on the Same Day

26. Specification 10 of Charge II alleges that PFC Manning impermissibly disclosed certain classified records in violation of Section 793(e). Specification 11 of Charge II alleges that PFC

Manning impermissibly disclosed a video relating to the national defense in violation of Section 793(e).

27. Though the Government alleges different date ranges for these two disclosures, in reality the classified records and the video were disclosed at the same time on the same day, 11 April 2010.² Therefore, the conduct alleged in Specifications 10 and 11 constitutes a single disclosure. The Government's attempt to break this single disclosure down into two disclosures constitutes an unreasonable multiplication of charges:

a. First, this motion serves as PFC Manning's objection to the unreasonable multiplication of charges, so this factor must be resolved in his favor. *See Paxton*, 64 M.J. at 491.

b. Second, Specifications 10 and 11 are directed at the same conduct: a single disclosure of certain classified records and a video. The specifications are not directed at distinctly separate conduct. *See Quiroz*, 55 M.J. at 338. Like the Government's impermissible breakdown of one larceny into two separate larcenies in *Gilchrist*, *see* 61 M.J. at 788-89, the Government here has impermissibly broken down a single disclosure into two separate disclosures. For the reasons stated in *Gilchrist*, this constitutes an unreasonable multiplication of charges. *See id.*; *see also Burris*, 21 M.J. at 82; *cf. Johnson*, 39 M.J. at 711.

c. Third, breaking down a single disclosure into two specifications, each alleging separate disclosures, misrepresents and exaggerates PFC Manning's criminality. *See Quiroz*, 55 M.J. at 338. Instead of being charged for the one disclosure, PFC Manning is being charged with two disclosures, even though the records referenced in Specification 10 and the video file referenced in Specification 11 were disclosed at the same time.

d. Fourth, this overcharging unreasonably increases PFC Manning's punitive exposure. *See Quiroz*, 55 M.J. at 338-39. Instead of facing a maximum ten year sentence for his alleged Section 793(e) violation (the single disclosure), PFC Manning faces two specifications, each containing a ten year maximum punishment. *See* 18 U.S.C. § 793(e) (containing maximum punishment of imprisonment for ten years). Doubling an accused's punitive exposure in this manner, as explained by the Navy-Marine Court of Criminal Appeals, constitutes an unreasonable multiplication of charges. *See Quiroz*, 57 M.J. at 586.

e. Finally, the Government's decision to multiply a single disclosure into two specifications itself demonstrates prosecutorial overreaching and abuse. Both the purpose and effect of this artificial splitting of one offense into two is to unnecessarily pile on the charges against PFC Manning to exaggerate his criminality and increase his punitive exposure. The principle of unreasonable multiplication of charges is primarily aimed at preventing such a piling on of charges and specifications. *See Quiroz*, 55 M.J. at 337.

28. For these reasons, this Court should determine that Specifications 10 and 11 of Charge II constitute an unreasonable multiplication of charges and should accordingly consolidate these specifications into one specification.

² PFC Manning's Primary SIPRNET Computer Forensic Report, Bates # 00211037-110, at 51-52; PFC Manning's Personal Computer Forensic Report, Bates # 00124283-362, at 49, 54-58, 65-68.

CONCLUSION

29. For the reasons articulated above, this Court should determine the following:

- a. that Specifications 4 and 5 of Charge II constitute an unreasonable multiplication of charges and accordingly dismiss Specification 4;
- b. that Specifications 6 and 7 of Charge II constitute an unreasonable multiplication of charges and accordingly dismiss Specification 6;
- c. that Specifications 4, 5, 6, and 7 constitute an unreasonable multiplication of charges and, in addition to the dismissals specified in a and b, consolidate Specifications 5 and 7 into one specification;
- d. that Specifications 8 and 9 of Charge II constitute an unreasonable multiplication of charges and accordingly dismiss Specification 8;
- e. that Specifications 12 and 13 of Charge II constitute an unreasonable multiplication of charges and accordingly dismiss Specification 12; and
- f. that Specifications 10 and 11 of Charge II constitute an unreasonable multiplication of charges and accordingly consolidate those specifications into one specification.

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

Appellate Exhibit 57
Attachments C and D
classified
"SECRET"

ordered sealed for Reason 2
Military Judge's Seal Order
dated 26 April 2012
stored in the classified
supplement to the original
Record of Trial

Appellate Exhibit 57
Attachments C and D
classified
"SECRET"

ordered sealed for Reason 2
Military Judge's Seal Order
dated 26 April 2012
stored in the classified
supplement to the original
Record of Trial

Appellate Exhibit 57

Attachment E

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 26 April 2012

stored in the classified

supplement to the original

Record of Trial

27 March 2012

MEMORANDUM FOR RECORD

SUBJECT: Security Expert Review of Defense Motions

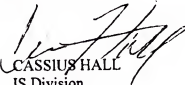
1. I hereby certify that I have reviewed the following Defense motions for the presence of classified information:

- a) Defense Motion to Dismiss the Specification of Charge I for Failure to State an Offense;
- b) Defense Motion to Dismiss Specification I of Charge II for Failure to State an Offense;
- and
- c) Defense Motion to Dismiss Based Upon Unreasonable Multiplication of Charges

I do not believe that any of these motions contain classified information or information that a reasonable person could believe to be classified.

2. The Unreasonable Multiplication of Charges motion does cite to classified attachments. However, these attachments will be provided separately from the motion.

3. The point of contact for this memorandum is the undersigned at [703-428-430].


CASSIUS HALL
IS Division
INSCOM G2

28 March 2012

MEMORANDUM FOR RECORD

SUBJECT: Security Expert Review of Defense Motion

1. I hereby certify that I have reviewed the following Defense motion for the presence of classified information:

a) Defense Motion to Dismiss [793 v3]

I do not believe that this motion contains classified information or information that a reasonable person could believe to be classified.

2. The point of contact for this memorandum is the undersigned at [703-428-4340].



CASSIUS HALL
IS Division
INSCOM G2

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

**GOVERNMENT RESPONSE
TO DEFENSE MOTION TO DISMISS
BASED UPON UNREASONABLE
MULTIPLICATION OF CHARGES**

12 April 2012

RELIEF SOUGHT

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny the defense motion to dismiss and/or consolidate specifications based upon the allegation they constitute an unreasonable multiplication of charges. In the alternative, the United States requests the Court defer ruling on this motion until after the presentation of evidence or after ruling on proposed defense motions to dismiss specifications charged as violations of 18 U.S.C. §793(e) and 18 U.S.C. §1030(a)(1). The United States also requests the Court make findings establishing the elements of the 18 U.S.C. §641, 18 U.S.C. §793(e), and 18 U.S.C. §1030(a)(1) offenses.

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the defense has the burden of persuasion on any factual issue the resolution of which is necessary to decide the motion. *Manual for Courts-Martial (MCM)*, United States, Rule for Courts-Martial (RCM) 905(c)(2) (2008). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

FACTS

The United States stipulates to the facts as set forth in the defense motion, except for the following statement: "The case has been referred to a general court-martial by the convening authority with a special instruction that the case is not a capital referral." The above-captioned case was referred to a general court-martial without special instructions.

WITNESSES/EVIDENCE

The United States requests this Court consider the following enclosures:

1. Enclosure 1 to Appellate Exhibit XV, (pp. 25-27 of the Continuation Sheet to DD Form 457)
2. Charge Sheet
3. SD Card Forensic Report

ELEMENTS

The United States requests this Court adopt the following elements for the specifications charging misconduct in violation of 18 U.S.C. §641, 18 U.S.C. §793(e), 18 U.S.C. §1030(a)(1):

18 U.S.C. §641

- (1) That the accused did [steal] [purloin] [knowingly convert] a [record] [thing of value];
- (2) That the [record] [thing of value] belonged to the United States government;
- (3) That the [record] [thing of value] was of a value of more than \$1,000;
- (4) That the taking by the accused was with the intent to deprive the United States government of the use or benefit of the property;
- (5) That, at the time, 18 U.S.C. §641 was in existence;
- (6) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

18 U.S.C. §793(e)

- (1) That the accused had possession of information relating to the national defense;
- (2) That the possession was unauthorized;
- (3) That the accused had reason to believe that such information could be used to [the injury of the United States] [the advantage of any foreign nation];
- (4) That the accused willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, the said information, to a person not entitled to receive it;
- (5) That, at the time, 18 U.S.C. §793(e) was in existence;
- (6) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

18 U.S.C. §1030(a)(1)

- (1) That the accused knowingly exceeded authorized access on a computer;

- (2) That the accused obtained information that has been determined by the United States government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of [national defense] [foreign relations];
- (3) That the accused willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, the said information, to a person not entitled to receive it;
- (4) That the accused had reason to believe that such information could be used to [the injury of the United States] [the advantage of any foreign nation];
- (5) That, at the time, 18 U.S.C. §1030(a)(1) was in existence;
- (6) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

LEGAL AUTHORITY AND ARGUMENT

RCM 307(c)(4) states that “[w]hat is substantially one transaction should not be made the basis for an unreasonable multiplication of charges against one person.” The Court of Appeals for the Armed Forces has endorsed a four-part test for a trial court to determine whether the Government has unreasonably multiplied charges:

- (1) Is each charge and specification aimed at distinctly separate criminal acts?
- (2) Does the number of charges and specifications misrepresent or exaggerate the accused’s criminality?
- (3) Does the number of charges and specifications unreasonably increase the accused’s punitive exposure?
- (4) Is there any evidence of prosecutorial overreaching or abuse in the drafting of the charges?

United States v. Campbell, 71 M.J. 19 (C.A.A.F. 2012) (citing *United States v. Quiroz*, 55 M.J. 334, 338); *United States v. Pauling*, 60 M.J. 91 (C.A.A.F. 2004). In considering whether there is an unreasonable multiplication of charges, courts must balance the factors, “with no single factor necessarily governing the result.” *Pauling*, 60 M.J. at 95. Ultimately, the doctrine is rooted in the traditional legal standard of “reasonableness” and is designed to address prosecutorial overreaching or abuse. See *Quiroz*, 55 M.J. at 338.

The defense argues that several specifications in this case violate the prohibition against unreasonable multiplication of charges. See Def. Mot. at 4. The United States disagrees. Analysis of the four factors articulated by the *Quiroz* court demonstrates that the specifications at

issue in this case do not constitute an unreasonable multiplication of charges for the reasons set forth below.

I. THE 18 U.S.C. §641 AND 18 U.S.C. §793(e) SPECIFICATIONS, TAKEN TOGETHER, DO NOT CONSTITUTE SUBSTANTIALLY ONE TRANSACTION.

A. The specifications are aimed at distinctly separate criminal acts.

The defense argues that each of the paired specifications (4 and 5; 6 and 7; 8 and 9) split one transaction into two specifications. See Def. Mot. at 5. Although the paired specifications relate to the same type of information – for example, Specifications 4 and 5 allege misconduct related to the “Combined Information Data Network Exchange Iraq database” – the paired specifications are aimed at distinctly separate criminal acts, as illustrated by comparing the elements of the offenses. See *Pauling*, 60 M.J. at 95 (referring to the court’s multiplicity analysis in deciding that the specifications at issue were aimed at distinctly separate criminal acts). In order to prove the accused violated 18 U.S.C. §641 – Specifications 4, 6, and 8 – the United States must establish that the accused stole, purloined, or knowingly converted (hereinafter “stole” or “theft” in general context) United States Government property. See 18 U.S.C. §641. In order to prove the accused violated 18 U.S.C. §793(e) – Specifications 5, 7, and 9 – the United States must establish that the accused communicated, delivered, or transmitted national defense information to a person not entitled to receive it. See 18 U.S.C. §793(e). In short, the 18 U.S.C. §641 offenses are aimed at the theft of United States Government-owned databases, while the gravamen of the 18 U.S.C. §793(e) offenses is that the accused transmitted national defense information to unauthorized persons. Each specification alleging a violation of 18 U.S.C. §641 is directed at misconduct independent of its paired specification alleging a violation of 18 U.S.C. §793(e). The accused could have committed a theft of government property without a corresponding unauthorized transmission, and vice versa. As such, the paired specifications are aimed at distinctly separate criminal acts.

The defense also argues the paired specifications cannot logically be separated because the element of “unauthorized possession” under 18 U.S.C. §793(e) could not be met without first stealing or knowingly converting the database charged. See Def. Mot. at 6. This type of argument has been consistently rejected by appellate courts considering unreasonable multiplication of charges in the larceny and false claims context. In *United States v. Chatman*, 2003 WL 25945959 (A. Ct. Crim. App. June 13, 2003) (unpublished), the Army Court of Criminal Appeals rejected the appellant’s claim that the specifications at issue were unreasonably multiplied because the proceeds of the false claims, supported in part by false receipts, were the subject of the larceny offense. *Chatman*, 2003 WL 25945959. The *Chatman* court held that “the Article 132, UCMJ, offenses have nothing to do with the gravamen of the larceny offense.” *Id.*; see also *United States v. Brumfield*, 2005 WL 2704969 (N-M. Ct. Crim. App. Oct. 12, 2005) (unpublished) (rejecting claim of unreasonable multiplication of charges and stating that the “larceny and fraud offenses were aimed at distinctly separate criminal acts—the fraud offenses were complete as soon as the false claims were sent to DFAS, while the larceny was not complete until the money was actually received”). Like the false claims in *Chatman* and *Brumfield*, the records stolen under 18 U.S.C. §641 exist separate and apart from the misconduct relating to transmission of those records to unauthorized persons under 18 U.S.C. §793(e).

Because each pair of specifications constitutes a distinctly separate criminal act from its counterpart, the first factor under *Quiroz* must be resolved in favor of the United States.

B. The number of charges and specifications do not misrepresent or exaggerate the accused's criminality.

Analysis of the second factor also favors the United States. Between Specifications 4, 6, 8, and 12 of Charge II, the accused is charged with the theft of more than 700,000 records from various government databases. *See* Charge Sheet. The defense argues that the number of specifications misrepresents and exaggerates the accused's criminality. In fact, the specifications accurately represent the crimes the accused committed. As the court stated in *United States v. Foster*, 40 M.J. 140, 144 (C.M.A. 1994), "there is prosecutorial discretion to charge the accused for the offense(s) which most accurately describe the misconduct and most appropriately punish the transgression(s)." Charging the accused with the transmission of some small amount of national defense information would ignore the conduct that makes this case so unique in its criminality. Specifications 4, 6, and 8 capture the theft of an unprecedented amount of government information arising from various sources, regardless of whether the information was transmitted to another.

C. The number of charges and specifications do not unreasonably increase the accused's punitive exposure.

Additionally, Specifications 4, 6, and 8 do not unreasonably increase the accused's punitive exposure. The specifications are aimed at distinct misconduct and the punitive exposure is commensurate with the nature of the offenses. Further, the accused is charged with Giving Intelligence to the Enemy, a violation of Article 104. *See* Charge I and its Specification. Because this case was not referred capital, the Article 104 charge carries a maximum penalty of confinement for life without eligibility for parole. Even assuming, *arguendo*, that the Article 104 specification is dismissed, the remedy requested by the defense – dismissal of Specifications 4, 6, and 8 – would reduce the accused's punitive exposure from a maximum of 170 years confinement to a maximum of 140 years confinement. The third factor must also be resolved in favor of the United States because the accused's punitive exposure has not been unreasonably increased. The accused was charged with the very specific offenses he committed.

D. There is no evidence of prosecutorial overreaching or abuse in the drafting of charges.

Finally, there is no evidence, and the defense has pointed to nothing in this regard, of prosecutorial overreaching or abuse in the drafting of these specific specifications. The defense relies on Charge II itself as an example of prosecutorial overreaching, but as demonstrated above, Specifications 4, 6, and 8 are aimed at distinctly separate criminal acts from their counterparts in Specifications 5, 7, and 9. The specifications as a whole are designed to account for the egregious conduct of the accused while deployed in a combat zone. The defense believes the use of 18 U.S.C. §641 in the area of "information relating to the national defense" pushes the statute to the edge of its permissible application. *See* Def. Mot. at 7. This claim was rejected by the Fourth Circuit in *United States v. Fowler*, 932 F.2d 306 (4th Cir. 1991).

In *Fowler*, the accused was a Department of Defense civilian who retired and worked for the Boeing Aerospace Company ("Boeing"). Using his security clearance, he obtained classified documents from the Department of Defense and the National Security Council and delivered them to Boeing. Charged under 18 U.S.C. §641 with both conveying records and converting information to his own use, Fowler unsuccessfully moved to dismiss on the ground that 18 U.S.C. §641 does not punish the acquisition of classified information. See *Fowler*, 932 F.2d at 309. He urged the court to adopt the separate view expressed by Judge Winter in *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980). *Id.* As the *Fowler* court noted, Judge Winter, without concurrence of the other members of the court, wrote that Congress did not intend for 18 U.S.C. §641 to apply to the theft of government information. *Id.* The Fourth Circuit disagreed, citing *United States v. Morison*, 844 F.2d 1057, 1077 (4th Cir. 1988) (finding no error in the conviction under 18 U.S.C. §641 for the conversion of secret Navy documents and photographs); *United States v. Carpenter*, 484 U.S. 19, 25 (1987) (holding that intangible nature of newspaper's confidential business information did not make it any less "property" protected by mail and wire fraud statutes); *United States v. Jeter*, 775 F.2d 670, 680-82 (6th Cir. 1985); *United States v. Girard*, 601 F.2d 69, 70-71 (2nd Cir. 1979). The court concluded that "information is a species of property and a thing of value," and that "conversion and conveyance of governmental information can violate section 641." *Fowler*, 932 F.2d at 311. In short, the prosecution's use of 18 U.S.C. §641 in this case is a valid application of the statute and not evidence of prosecutorial overreaching or abuse as the defense claims.

II. SPECIFICATIONS 12 AND 13 OF CHARGE II, TAKEN TOGETHER, DO NOT CONSTITUTE SUBSTANTIALLY ONE TRANSACTION.

A. The specifications are aimed at distinctly separate criminal acts.

Addressing the four *Quiroz* factors at issue, Specifications 12 and 13 of Charge II do not constitute an unreasonable multiplication of charges. Like the paired 18 U.S.C. §641 and §793(e) offenses, Specifications 12 and 13 relate to information owned by the same organization—the Department of State. However, the specifications are aimed at distinctly separate criminal acts—as illustrated by comparing the elements of the offenses. In order to prove the accused violated 18 U.S.C. §641, the United States must establish that the accused stole or knowingly converted United States Government property. See 18 U.S.C. §641. In order to prove the accused violated 18 U.S.C. §1030(a)(1), the United States must establish that the accused willfully communicated, delivered, or transmitted to unauthorized persons "information that has been determined by the United States government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations." See 18 U.S.C. §1030(a)(1). Again, the 18 U.S.C. §641 offense is aimed at the theft of particular United States Government-owned database, while an 18 U.S.C. §1030(a)(1) offense cannot be completed without the transmission of specific classified information to unauthorized persons. The first *Quiroz* factor must be resolved in favor of the United States. Specifications 12 and 13 are directed at distinctly separate criminal acts and stand completely on their own.

B. The number of charges and specifications do not misrepresent or exaggerate the accused's criminality.

Analysis of the third *Quiroz* factor also favors the United States. The defense argues that including Specification 12 misrepresents and exaggerates the accused's criminality, when in fact Specification 12 accurately captures the varied misconduct of the accused. As the court stated in *Foster*, "[T]here is prosecutorial discretion to charge the accused for the offense(s) which most accurately describe the misconduct and most appropriately punish the transgression(s)." *Foster*, 40 M.J. at 144. Charging the accused with exceeding authorized access on a computer and transmitting some small amount of classified information would ignore the conduct that makes this case so unique in its criminality. Specification 12 captures the theft or knowing conversion of an entire database worth of government information. It does not misrepresent or exaggerate the accused's misconduct, but attempts to account for it.

C. The number of charges and specifications do not unreasonably increase the accused's punitive exposure.

Additionally, the specifications at issue do not unreasonably increase the accused's punitive exposure. The specifications are aimed at distinct misconduct and the punitive exposure is commensurate with the nature of the offenses. Further, the accused is charged with Giving Intelligence to the Enemy, a violation of Article 104. *See* Charge I and its Specification. Because this case was not referred capital, the Article 104 charge carries a maximum penalty of confinement for life without eligibility for parole. Even assuming, *arguendo*, that the Article 104 specification is dismissed, the remedy requested by the defense – dismissal of Specification 12 – would only reduce the accused's punitive exposure from a maximum of 170 years confinement to a maximum of 160 years confinement. The fourth factor must also be resolved in favor of the United States because the accused's punitive exposure has not been unreasonably increased by including Specification 12. Specification 12 does increase the accused's punitive exposure, but only as a reflection of the accused's misconduct in this case.

D. There is no evidence of prosecutorial overreaching or abuse in the drafting of charges.

Finally, there is no evidence, and the defense has pointed to nothing in this regard, of prosecutorial overreaching or abuse in the drafting of these specific specifications. The defense relies on "the way in which Specifications 12 and 13 have been drafted." Def. Mot. at 9. As discussed above with respect to the other *Quiroz* factors, the 18 U.S.C. §641 offense and the 18 U.S.C. §1030(a)(1) offense are aimed at distinctly separate criminal acts, occurring at different times, and designed to account for the egregious conduct of the accused while deployed in a combat zone. Additionally, the defense further argues there is prosecutorial overreaching or abuse in this case because 18 U.S.C. §1030(a)(1) was enacted to "rectify the deficiencies of using 18 U.S.C. §641 to combat computer misuse." Def. Mot. at 10. The article relied upon by the defense does not say this, nor does the defense cite any legislative history to that effect. Professor Kerr's article is concerned with the deficiencies in using 18 U.S.C. §641 for computer crimes when it is difficult to define the *res*. Orin Kerr, *The Limits of Computer Conversion: United States v. Collins*, 9 *Harvard Journal of Law & Technology* 205, 211 (1996). In this case, the *res* is very clear—the wholesale theft of government information. Ironically, Professor Kerr discusses the *Collins* case to suggest 18 U.S.C. §641 is ill-suited to address computer conversion or misappropriation of intangible property, although the facts would pose similar problems for a

prosecution under 18 U.S.C. §1030(a)(1). The defendant in *Collins* was using his government computer to produce a newsletter for personal reasons, not obtaining classified information or obtaining other information from any department or agency of the United States. See 18 U.S.C. §1030(a)(1) and (a)(2).

III. SPECIFICATIONS 4, 5, 6, AND 7 OF CHARGE II ARE DIRECTED AT CONDUCT THAT OCCURRED ON SEPARATE DAYS AND DO NOT CONSTITUTE AN UNREASONABLE MULTIPLICATION OF CHARGES.

The defense requests this Court dismiss and/or consolidate Specifications 4, 5, 6, and 7 of Charge II, leaving only one specification alleging a violation of 18 U.S.C. §793(e), based on the assertion that the specifications split the same transaction into multiple component parts. As discussed at length in Section I above, the conduct alleged by Specifications 4, 5, 6, and 7 of Charge II cannot be categorized as substantially one transaction. See *supra* Section I.

The defense argues that all four of the specifications are directed at conduct that occurred on the same day. Def. Mot. at 11. The evidence and a plain reading of the specifications contradict this assertion. See Charge Sheet. According to the forensic examination of the accused's Secure Digital (SD) card¹, the theft of the Combined Information Data Network Exchange Iraq database and the Combined Information Data Network Exchange Afghanistan database likely occurred on separate days, as evidenced by the "last written"² dates of the "afg_events.csv" file (8 January 2010) and the "irq_events.csv" file (5 January 2010). See Enclosure 3 at 9-10. The "afg_events.csv" file contains the records that are the subject of Specification 6. The "irq_events.csv" file contains the records that are the subject of Specification 4. Similarly, the forensic examination of the SD card indicates the transmission of the databases likely occurred sometime after 26 January 2010, because the accused was at his aunt's residence on leave and the compilation file ("yada.tar.bz2.nc"), containing the "afg_events.csv" and "irq_events.csv" sub-files, was created on 30 January 2010. See Enclosure 3 at 6-10. Thus, aside from the date ranges specified in the specifications themselves, the evidence clearly indicates that the misconduct charged in Specifications 4, 5, 6, and 7 of Charge II occurred on separate days. Each specification is directed at conduct independent of the conduct in the other specifications. The specifications do not constitute substantially one transaction as the defense has alleged.

¹ An SD card is a memory card developed for use in portable devices. They have become a widespread means of storing several gigabytes of data in a small device.

² The "last written" date field in Encase indicates the date the digital file was last modified on a media device or hard drive. Encase is a computer forensics product produced by Guidance Software used to analyze digital media by law enforcement agencies.


IV. SPECIFICATIONS 10 AND 11 OF CHARGE II ARE DIRECTED AT CONDUCT THAT OCCURRED ON SEPARATE DAYS AND DO NOT CONSTITUTE AN UNREASONABLE MULTIPLICATION OF CHARGES.

The defense asserts that Specifications 10 and 11 of Charge II are directed at a single disclosure of classified records and a video. Def. Mot. at 13. However, the defense acknowledges the difference between the two specifications—that as alleged, the disclosure of the classified records and the video occurred months apart. Furthermore, the “reality” the defense speaks of—that the classified records and the video were disclosed at the same time on the same day—is contradicted by the findings of the Article 32 investigating officer, who cited the Government’s evidence that (1) an individual named Jason Katz was in possession of the video as early as 15 December 2009, and (2) WikiLeaks was in possession of the video as early as 8 January 2010. See Enclosure 1. Considering the time periods of the specifications themselves and the evidence presented at the Article 32, Specifications 10 and 11 of Charge II are different transactions aimed at distinctly separate criminal acts.

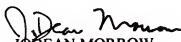
Additionally, the inclusion of Specification 11 of Charge II is not unreasonable and does not misrepresent or exaggerate the accused’s criminality; rather, it accurately represents the misconduct of the accused by charging him with transmitting national defense information to the WikiLeaks organization as early as 1 November 2009. See Charge Sheet. Finally, the question of when the video was transmitted should be left to the trier of fact. If, as the defense asserts, the classified records in Specification 10 were transmitted to an unauthorized person on the same day as the video in Specification 11, the panel or military judge can find the accused not guilty of Specification 11.

CONCLUSION

For the reasons stated above, the United States requests the Court DENY the defense motion to dismiss and/or consolidate specifications as an unreasonable multiplication of charges. If the Court is inclined to consider any specifications to be unreasonably multiplied, the United States requests the Court defer ruling on a remedy until after the presentation of evidence or after ruling on defense motions to dismiss the specifications charged as violations of 18 U.S.C. §793(e) and 18 U.S.C. §1030(a)(1).


JODEAN MORROW
CPT, JA
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 12 April 2012.


JODEAN MORROW
CPT, JA
Trial Counsel

Appellate Exhibit 58
Enclosure 1
has been entered into the
record as
Appellate Exhibit 15
Enclosure 1

Appellate Exhibit 58
Enclosure 2
is the charge sheet

Appellate Exhibit 58

Enclosure 3

13 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army, xxx-xx-)

Headquarters and Headquarters Company, U.S.)

Army Garrison, Joint Base Myer-Henderson Hall,)

Fort Myer, VA 22211)

**DEFENSE MOTION TO
DISMISS SPECIFICATION 1
OF CHARGE II FOR FAILURE
TO STATE AN OFFENSE**

DATED: 29 March 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 907(b)(1)(B), requests this Court to dismiss Specification 1 of Charge II for failure to state a cognizable offense under Article 134 because Specification 1 of Charge II, as currently drafted, is preempted by Article 104 or, in the alternative, because Specification 1 of Charge II must be charged as a violation of Article 92 since there is a lawful order or regulation prohibiting the unauthorized possession and dissemination of classified information.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. The Defense, as the moving party, bears the burden of this motion by a preponderance of the evidence pursuant to R.C.M. 905(c).

FACTS

3. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of conduct prejudicial to good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting government property, and two specifications of knowingly exceeding authorized access to a government computer, in violation of Articles 92, 104, and 134, Uniform Code of Military Justice (UCMJ), 10 U.S.C. §§ 892, 904, 934 (2010). The case has been referred to a general court martial by the convening authority with a special instruction that the case is not a capital referral.

4. In Specification 1 of Charge II, the Government pleads that PFC Manning “wrongfully and wantonly caused to be published on the internet intelligence belonging to the United States government, having knowledge that intelligence published on the internet is accessible to the enemy” Additionally, in the Specification of Charge I, the Government pleads that PFC Manning “between on or about 1 November 2009 and on or about 27 May 2010, without proper authority knowingly gave intelligence to the enemy, through indirect means.” On 14 February 2012, the Defense, pursuant to R.C.M. 906(b)(6), moved this Court to direct the Government to respond to a bill of particulars in the subject case on the grounds that it was necessary for PFC Manning to understand the charges against him so that he could adequately prepare his defense and not be subject to unfair surprise at trial. The Government’s particulars in response to the Specification of Charge I indicated that its theory of knowingly giving intelligence to the enemy was “by transmitting certain intelligence, specified in a separate classified document, to the enemy through the WikiLeaks website.” *See* Government Bill of Particulars Response. The Government also stated that its theory of indirect means was that PFC Manning gave the charged intelligence to “the WikiLeaks website.” *Id.* Additionally, the Government’s particulars in response to Specification 1 of Charge II was that PFC Manning wrongfully and wantonly cause intelligence to be published on the Internet “by leaking thousands of documents gathered from the SIPRNET, including several databases, to the WikiLeaks organization.” *Id.* The Defense maintains that Specification 1 of Charge II should be dismissed because it is preempted by Article 104. In the alternative, the Defense argues that Specification 1 of Charge II should be dismissed because it must be charged as a violation of Article 92 – and not as a violation of Article 134 – since there is a lawful general order or regulation covering PFC Manning’s alleged conduct that forms the factual basis for Specification 1 of Charge II, namely, the unauthorized possession and dissemination of classified information.

WITNESSES/EVIDENCE

5. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this court to consider the following evidence in support of the Defense’s motion.

- a. Charge Sheet;
- b. Continuation of DD Form 457.

LEGAL AUTHORITY AND ARGUMENT

- A. **Specification 1 of Charge II Should be Dismissed Because it is Preempted by Article 104**

6. The Defense submits that Specification 1 of Charge II fails to state a cognizable offense because it is preempted by Article 104. Accordingly, the specification should be dismissed.

7. Article 104 punishes “[a]ny person who – (1) aids, or attempts to aid, the enemy with arms, ammunition, supplies, money, or other things; or (2) without proper authority, knowingly harbors or protects or gives intelligence to, or communicates or corresponds with or holds any intercourse with the enemy, either directly or indirectly[.]” 10 U.S.C. § 904. Article 134, by contrast, applies to offenses “not specifically mentioned in [the UCMJ.]” *Id.* § 934.

8. The Court of Military Appeals has defined the doctrine of preemption as “the legal concept that where Congress has occupied the field of a given type of misconduct by addressing it in one of the specific punitive articles of the code, another offense may not be created and punished under Article 134, UCMJ, simply by deleting a vital element.” *United States v. Kick*, 7 M.J. 82, 85 (C.M.A. 1979). The preemption doctrine is described in paragraph 60(c)(5)(a) of the Manual for Courts-Martial (MCM), which provides, in pertinent part:

The preemption doctrine prohibits application of Article 134 to conduct covered by Articles 80 through 132. For example, larceny is covered in Article 121, and if an element of that offense is lacking – for example, intent – there can be no larceny or larceny-type offense, either under Article 121 or, because of preemption, under Article 134. Article 134 cannot be used to create a new kind of larceny offense, one without the required intent, where Congress has already set the minimum requirements for such an offense in Article 121.

MCM, para. 60(c)(5)(a). Courts apply a two-pronged test to determine whether an Article 134 charge is preempted by another Article in any given case. First, it must be shown that Congress “indicate[d] through direct legislative language or express legislative history that particular actions or facts are limited to the express language of an enumerated article, and may not be charged under Article 134, UCMJ.” *United States v. Anderson*, 68 M.J. 378, 387 (C.A.A.F. 2010); *see Kick*, 7 M.J. at 85; *United States v. Wright*, 5 M.J. 106, 110-11 (C.M.A. 1978). Second, it must be established that the offense charged under Article 134 is composed of a “residuum of elements” of an enumerated offense under the UCMJ. *Wright*, 5 M.J. at 111; *see Kick*, 7 M.J. at 85. Both prongs are satisfied by the Government’s use of Article 134 in the instant case.

9. Congress clearly intended Article 104 to occupy the field of aiding or communicating with the enemy. Article 104 uses very broad language to accomplish this intent; the Article punishes anyone who aids, attempts to aid, knowingly harbors, protects, gives intelligence to, communicates with, corresponds with, or holds any intercourse with the

enemy. 10 U.S.C. § 904. Not only does Article 104 prohibit each and every one of these acts, a person can violate this Article “either directly or indirectly[.]” *Id.* Through this “direct legislative language,” *Anderson*, 68 M.J. at 387, Congress has clearly demonstrated its intent for Article 104 “to cover a class of offenses in a complete way.” *Kick*, 7 M.J. at 85. Therefore, the first prong of the preemption inquiry is satisfied by the all encompassing language of Article 104.

10. Additionally, the Article 134 specification that the Government has attempted to charge in this case is simply a residuum of most of the elements required for an Article 104 prosecution. For the reasons fully articulated in the Defense’s Article 104 Motion to Dismiss, the Government’s Article 104 charge – that PFC Manning indirectly gave intelligence information to the enemy by publishing it on the internet with the knowledge that it could be accessed by the enemy – fails to state a cognizable offense under Article 104 because it does not allege the requisite intent to aid the enemy. *See* Defense Motion to Dismiss the Specification of Charge I for Failure to State an Offense. The Government has simply used Article 134 in an effort to rectify its inability to allege the requisite criminal intent under Article 104. However, the Government is not permitted to utilize Article 134 to circumvent the intent requirement of Article 104 in this manner. As mentioned above, the Government has alleged that PFC Manning violated Article 134 by “wrongfully and wantonly causing to be published on the internet intelligence belonging to the United States, thereby providing such intelligence to persons not entitled to receive it, having knowledge that intelligence published on the internet is accessible to the enemy.” However, this specification essentially alleges an Article 104 violation – indirectly giving intelligence to the enemy – without alleging any corresponding *mens rea*.

11. This is precisely the evil that the preemption doctrine was designed to combat. The first case enunciating the preemption doctrine in the UCMJ context, *United States v. Norris*, perfectly illustrates this point. In that case, the accused was charged with larceny and wrongful appropriation under Article 121 and wrongful taking under Article 134. *United States v. Norris*, 8 C.M.R. 36, 37-38 (C.M.A. 1953). The accused was initially found guilty of wrongful appropriation and wrongful taking, but on appeal the board of review held that the law officer had erred in not instructing on the effect of intoxication on specific intent. *Id.* at 38. The board remedied this defect by vacating the wrongful appropriation conviction and affirming the wrongful taking conviction under Article 134, as the offenses charged under Article 121 required a specific intent to deprive the owner of the property, either permanently or temporarily, and the wrongful taking charge required only a general criminal intent. *Id.* The Court of Military Appeals reversed, holding that “there is no offense known as ‘wrongful taking’ requiring no element of specific intent, embraced by Article 134 of the Code.” *Id.* at 40. The Court reasoned that:

Article 134 should generally be limited to military offenses and those crimes not specifically delineated by the punitive articles . . . We cannot

grant to the services unlimited authority to eliminate vital elements from common law crimes and offenses expressly defined by Congress and permit the remaining elements to be punished as an offense under Article 134.

Id. at 39. Just as the Government was not permitted in *Norris* to use Article 134 to create an Article 121-type offense when it was unable to prove the requisite intent under Article 121, so too should the Government not be permitted here to use Article 134 to create an Article 104-type offense when it is unable to prove the requisite intent under Article 104. *See id.* at 39-40; *see also* MCM, para. 60(c)(5)(a). As Specification 1 of Charge II is currently drafted, this is precisely what the phrase “having knowledge that intelligence published on the internet is accessible to the enemy” seeks to accomplish. Thus, this specification should be dismissed, as it is preempted by Article 104.

12. The result in *Anderson* does not foreclose the preemption question in this case. The accused in *Anderson* provided emails including “comprehensive information about the number of soldiers in his unit, their training programs, and the precise location to which his unit would be deploying” to a person he believed to be a “Muslim extremist,” who in reality was a concerned American citizen attempting to thwart terrorist activities. 68 M.J. at 381. The accused also met with undercover FBI agents whom he believed to be Al Qaeda operatives and disclosed to them “computer diskettes containing classified information on the vulnerabilities of various military vehicles, the vulnerabilities of his unit as they travelled to Iraq, and other sensitive information.” *Id.* As a result of his conduct, the accused was charged with, and convicted of, attempting to give intelligence information to the enemy, attempting to communicate with the enemy, and attempting to aid the enemy, all in violation of Articles 80 and 104, and of “wrongfully and dishonorably providing information to military personnel whom he believed were terrorists, which was conduct prejudicial to good order and discipline and of a nature to bring discredit upon the armed forces,” in violation of Article 134. *Id.* at 380.

13. On appeal, the accused contended, *inter alia*, that Article 104 preempted the Article 134 offense in his case. *Id.* at 386. The Court of Appeals for the Armed Forces rejected the accused’s preemption argument. *Id.* at 387. The Court first reasoned that “the legislative history of Article 104, UCMJ, does not clearly indicate that Congress intended for offenses similar to those at issue to only be punishable under Article 104, UCMJ, to the exclusion of Article 134, UCMJ.” *Id.* The Court then observed that “while the two charges in this case have parallel facts, as charged they are nonetheless directed at distinct conduct.” *Id.* The Court elaborated:

The Article 104, UCMJ, charge was directed at [accused’s] attempt to aid the enemy directly. The Article 134, UCMJ, charge was directed towards the distribution of sensitive material to individuals not authorized to receive it—in this case Criminal Investigation Command agents posing as the enemy, but the reasoning could just as easily be applied to the

distribution of information to individuals who are not necessarily the enemy, such as a newspaper reporter, or for that matter the private citizen who first encountered [accused] on the “Brave Muslim” website. Unlike Article 104, UCMJ, the general offense as charged prohibits the dissemination of the information regardless of the intent behind that dissemination. If this distinction was not permissible in light of Article 104, UCMJ, Congress was free to clearly state that Article 104, UCMJ, supersedes Article 134, UCMJ, in this context.

Id.

14. Here, unlike in *Anderson*, the Article 104 Specification of Charge I and the Article 134 Specification (Specification 1) of Charge II are not aimed at distinct conduct, but rather are aimed at the exact same conduct – PFC Manning’s alleged publication of United States intelligence information on the internet. Moreover, the Article 134 Specification in the instant case is not simply directed “towards the distribution of sensitive material to individuals not authorized to receive it[.]” as was the Article 134 Specification in *Anderson*. *Id.* Instead, the Government in this case has broadened the reach of Article 134 by including the phrase “having knowledge that intelligence published on the internet is accessible to the enemy” in the Article 134 Specification. By grafting this phrase into the Article 134 Specification, the Government has vitiated the distinction that the *Anderson* Court deemed crucial to its finding of no preemption: that the Article 104 charge was directed toward the accused’s attempt to aid the enemy directly and the Article 134 charge was solely directed towards the dissemination of the information, regardless of the purpose/knowledge behind that dissemination. *See id.* By contrast, the Government here has directed the Article 134 charge and Article 104 charge at identical conduct and extended the reach of Article 134 beyond where it must remain contained: solely at the dissemination of the information to one not authorized to receive it. *Id.*

15. Additionally, the *Anderson* Court’s statement that “the legislative history of Article 104, UCMJ, does not clearly indicate that Congress intended for offenses similar to those at issue to only be punishable under Article 104, UCMJ, to the exclusion of Article 134, UCMJ[.]” must be read in context. *Id.* (emphasis supplied). In *Anderson*, the Article 134 charge was directed solely at the accused’s dissemination of information to those not authorized to receive it; it was immaterial to that charge whether he knew that the enemy could access or utilize the information he provided. *Id.* Thus, it is hardly surprising that the *Anderson* Court was unable to find any legislative history to clearly indicate that Congress intended to preempt Article 134 prosecutions for unauthorized dissemination of classified information. In the instant case, however, PFC Manning’s alleged knowledge of the fact that the information could be accessed by the enemy appears to be central to the Article 134 Specification. The all-encompassing language of Article 104 clearly evidences Congress’s intent to limit the prosecution of all efforts to aid or communicate

with the enemy to Article 104, and to preclude any Article 134 prosecutions of such conduct.

16. For these reasons, Specification 1 of Charge II, as currently charged, is preempted by Article 104. Accordingly, that specification should be dismissed.

B. Specification 1 of Charge II Should be Dismissed Because the Facts Alleged Must be Charged as a Violation of Article 92 and not as a Violation of Article 134

17. In the alternative, the Defense submits that the Government fails to state an Article 134 offense against PFC Manning because it cannot lawfully charge an accused with an Article 134 offense when the charged conduct violates a punitive lawful general order or regulation. In such a situation, that conduct must be charged, if at all, as a violation of Article 92. In the instant case, PFC Manning's alleged conduct is claimed to be in violation of a lawful general order or regulation concerning the unauthorized possession and dissemination of classified information. Therefore, the Government cannot charge PFC Manning with an Article 134 violation and Specification 1 of Charge II must accordingly be dismissed.

18. Article 134 provides in full as follows:

Though not specifically mentioned in this chapter, all disorders and neglects to the prejudice of good order and discipline in the armed forces, all conduct of a nature to bring discredit upon the armed forces, and crimes and offenses not capital, of which persons subject to this chapter may be guilty, shall be taken cognizance of by a general, special, or summary court-martial, according to the nature and degree of the offense, and shall be punished at the discretion of that court.

10 U.S.C. § 934 (emphasis supplied). Article 92 provides for punishment of any person subject to the UCMJ who "(1) violates or fails to obey any lawful general order or regulation; (2) having knowledge of any other lawful order issued by a member of the armed forces, which it is his duty to obey, fails to obey the order; or (3) is derelict in the performance of his duties[.]" *Id.* § 892.

19. The Air Force Court of Criminal Appeals in *United States v. Borunda* recently clarified the interplay between Articles 92 and 134 where the invocation of Article 134 is premised on the same conduct that would support an Article 92 charge. *See* 67 M.J. 607 (2009). Citing *United States v. Caballero*, 49 C.M.R. 594 (C.M.A. 1975), the *Borunda* court held that "when a lawful general order or regulation proscribing [certain conduct] exists, an order or regulation which by definition is punitive, the [proscribed conduct], if charged, will only survive legal scrutiny as a violation of Article 92(1), UCMJ, and not as

a violation of Article 134, UCMJ.” *Borunda*, 67 M.J. at 609 (footnote omitted) (emphasis supplied). The court upheld the use of Article 134 to prosecute an accused for possession of drug paraphernalia where no lawful general order or regulation proscribed such possession, concluding that “in the absence of a lawful general order or regulation, charging officials are at liberty to charge the possession of drug paraphernalia as a violation of Article 92(3), UCMJ, or Article 134, UCMJ.” *Id.* (footnotes omitted).

20. The *Borunda* court’s holding is supported by both case law and commentary. In *Caballero*, for instance, the Court of Military Appeals addressed the issue of “whether the wrongful and unlawful possession of narcotic paraphernalia on-post, absent any regulation or general order prohibiting that conduct *so as to render any violation thereof an offense under Article 92, UCMJ*, can be properly charged or alleged as an offense under clause 1 of Article 134.” 49 C.M.R. at 595 (emphasis supplied). The Court in *Caballero* reversed the accused’s conviction under Article 134 for wrongful possession of narcotic paraphernalia, finding that the specification failed to allege an offense. *Id.* at 597. Specifically, the Court declined the Government’s request to construe Article 134 broadly enough to cover the charged conduct:

Since this Court has long recognized and held that the possession of narcotic paraphernalia might otherwise be properly prosecuted as an Article 92 violation, where such an order or regulation exists, we find no demonstrated need to expand the reach of Article 134, beyond that which already exists, to cover an offense such as this.

Id. Thus, *Caballero* supports *Borunda*’s holding that a court must not sustain an Article 134 prosecution under the first or second clause where the conduct underlying that prosecution also violates a lawful general order or regulation.

21. Additionally, the MCM provides that “[i]f any conduct [falling within Article 134’s reach] is specifically made punishable by another article of the code, it must be charged as a violation of that article.” MCM, para. 60(c)(1). More to the point, the MCM further explains that “[m]any customs of the service are now set forth in regulations of the various armed forces. Violations of these customs *should be charged under Article 92* as violations of the regulations in which they appear if the regulation is punitive.” *Id.* para. 60(c)(2)(b) (emphasis supplied); *see also United States v. Henderson*, 32 M.J. 941, 948 (N-M.C.M.R. 1991) (Lawrence, J., concurring) (“[T]he existence of an established custom of the military service may satisfy the notice requirement. The existence of the custom must be proved. If the custom is set forth in a punitive regulation or order, violation of it should be charged under Article 92.”).

22. Relying on an earlier version of the MCM containing similar language, Judge Ferguson of the Court of Military Appeals observed that:

“When an offense is specifically defined in a particular punitive article, it ordinarily should be charged under that article rather than under Article 134, the general article.”

Article 92 is one of the punitive articles of the Code . . . and regulations promulgated thereunder must be considered, when charging a violation of the Code, before recourse may be had to the use of Article 134.

United States v. Walter, 43 C.M.R. 207, 212 (C.M.A. 1971) (Ferguson, J., dissenting) (quoting MCM, para. 27 (1969 ed.)). Judge Ferguson cautioned that “Article 134 was not intended by Congress to apply in areas otherwise the subject of specific attention in Articles of the Uniform Code.” *Id.* (quoting *United States v. Hallett*, 15 C.M.R. 378, 382 (C.M.A. 1954)).

23. Along similar lines, one commentator has remarked that “Article 92 makes the General Articles [*i.e.* Articles 133 and 134] unnecessary[.]” Note, *Taps for the Real Catch-22*, 81 Yale L. J. 1518, 1541 (1972); *see also Parker v. Levy*, 417 U.S. 733, 788 n.2 (1974) (Stewart, J., dissenting) (citing 81 Yale L. J. 1518 in support of the proposition that Article 92, and not Article 134, should be utilized for failure to obey lawful orders); *cf. United States v. Harwood*, 46 M.J. 26, 29 (C.M.A. 1997) (Cox, C.J., concurring) (“Article 134 has always been understood as a residual provision rather than a redundant one.”).¹

24. Here, the facts alleged by the Government bring this case squarely within the rule announced in *Borunda*. PFC Manning is alleged to have wrongfully and wantonly caused to be published on the internet United States intelligence information with the knowledge that such information is accessible to the enemy. At the time of PFC Manning’s alleged unlawful actions, the United States Army had a punitive lawful general order or regulation proscribing the unauthorized possession and distribution of classified information. *See* Army Regulation 380-5, Paragraph 1-21a (stating that Department of Army personnel will be subject to sanctions if they knowingly, willfully, or negligently disclose classified or sensitive information to unauthorized persons). If the Government’s evidence is to be believed, PFC Manning’s actions constitute a violation of that lawful general order or regulation. *See* MCM, para. 16(b)(1) (stating the elements of a successful Article 92(1) prosecution: “(a) That there was in effect a certain lawful

¹ The resolution of this issue is not controlled by *United States v. McGuinness*, wherein the Court of Military Appeals determined that “prosecution of violations of 18 U.S.C. § 793(e) under Clause 3 of Article 134 is not preempted by Article 92.” 35 M.J. 149, 152 (C.M.A. 1992). The rule announced in *Borunda* in no way relies on the preemption doctrine. *See Borunda*, 67 M.J. at 609. Additionally, while the conduct supporting the Article 134 charge (brought under clause 3) in *McGuinness* was the violation of a federal statute, *see* 35 M.J. at 152, the alleged conduct supporting the Article 134 specification and charge (brought under clause 1 or 2) in the instant case is PFC Manning’s alleged wrongful and wanton publication on the internet of United States intelligence information, with the knowledge that information placed on the internet is accessible to the enemy. Thus, *McGuinness* is inapposite to the question of the propriety of the Government’s Article 134 specification and charge in this case.

general order or regulation; (b) That the accused had a duty to obey it; and (c) That the accused violated or failed to obey the order or regulation.”). Therefore, under the rule outlined in *Borunda*, the Government must charge this conduct, if at all, as a violation of Article 92; it cannot charge the conduct as a violation of Article 134. *See* 67 M.J. at 609.

25. Thus, because the Government cannot lawfully charge PFC Manning with a violation of Article 134 for conduct that is chargeable only under Article 92, the Government does not state a cognizable Article 134 offense against PFC Manning. Accordingly, Specification 1 of Charge II should be dismissed.

CONCLUSION

26. Wherefore, in light of the foregoing, the Defense requests this Court dismiss Specification 1 of Charge II for failure to state an offense because Specification 1 of Charge II, as currently drafted, is preempted by Article 104 or, in the alternative, because Specification 1 of Charge II must be charged as a violation of Article 92 since there is a lawful order or regulation prohibiting the unauthorized possession and dissemination of classified information.

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

28 March 2012

MEMORANDUM FOR RECORD

SUBJECT: Security Expert Review of Defense Motion

1. I hereby certify that I have reviewed the following Defense motion for the presence of classified information:

a) Defense Motion to Dismiss [793 v3]

I do not believe that this motion contains classified information or information that a reasonable person could believe to be classified.

2. The point of contact for this memorandum is the undersigned at [703-428-4340].



CASSIUS HALL
IS Division
INSCOM G2

27 March 2012

MEMORANDUM FOR RECORD

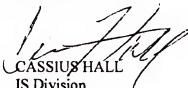
SUBJECT: Security Expert Review of Defense Motions

1. I hereby certify that I have reviewed the following Defense motions for the presence of classified information:

- a) Defense Motion to Dismiss the Specification of Charge I for Failure to State an Offense;
- b) Defense Motion to Dismiss Specification I of Charge II for Failure to State an Offense;
- and
- c) Defense Motion to Dismiss Based Upon Unreasonable Multiplication of Charges

I do not believe that any of these motions contain classified information or information that a reasonable person could believe to be classified.

- 2. The Unreasonable Multiplication of Charges motion does cite to classified attachments. However, these attachments will be provided separately from the motion.
- 3. The point of contact for this memorandum is the undersigned at [703-428-430].


CASSIUS HALL
IS Division
INSCOM G2

From: David Coombs
To: Lund, Denise R. COL MIL USA OTIAG
Cc: "Kemkes, Matthew J MAJ USARMY (US)"; "Bouchard, Paul R. CPT USARMY (US)"; "Santiago, Melissa S CW2 USARMY (US)"; "Morrow III, JoJoan. CPT USA JFHQ-NCR/MDW SJA"; "Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA"; "Wbyle, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA"; "Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA"; "ashden.fein@us.army.mil"; "Prather, Jay R. CIV (US)"; "Williams, Patricia. CIV JFHQ-NCR/MDW SJA"; "Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA"; "dashawn.jefferson@conus.army.mil"; "CASSIUS.HALL@MILARMY.MIL"; "Ganiel, Charles J. CIV (US)"; "Joshua Tooman"
Subject: Defense Motions
Date: Thursday, March 29, 2012 3:43:41 PM
Attachments: [Def. Article 104 Motion.pdf](#)
[Def. Article 104 Motion.doc](#)
[Attachment A.docx](#)
[Def. Article 134 Motion.pdf](#)
[Def. Article 134 Motion.doc](#)
[Def. UMC Motion.pdf](#)
[Def. UMC Motion.doc](#)
[Security Expert Review.pdf](#)

Ma'am,

I have attached PDF and Word versions of the following motions:

- a) Defense Motion to Dismiss The Specification of Charge I for Failure to State an Offense along with Attachment A;
- b) Defense Motion to Dismiss Specification 1 of Charge II for Failure to State an Offense; and
- c) Defense Motion to Dismiss Based Upon Unreasonable Multiplication of Charges (the Government will be sending the referenced classified attachments to the Court and Mr. Prather).

In addition to the attached motions, the Defense has attached the review of each motion completed by its Security Expert - Mr. Cassius Hall.

v/r
David

David E. Coombs, Esq.
Law Office of David E. Coombs
11 South Angell Street, #317
Providence, RI 02906
Toll Free: 1-800-588-4156
Local: (508) 689-4616
Fax: (508) 689-9282
coombs@armycourt martialdefense.com
www.armycourt martialdefense.com

Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

Prosecution Response to

Defense Motion to Dismiss Specification 1
of Charge II for Failure to
State an Offense

12 April 2012

RELIEF SOUGHT

The prosecution respectfully requests the Court deny the Defense Motion to Dismiss Specification 1 of Charge II for Failure to State an Offense (the "Defense Motion") because Specification 1 of Charge II (the "Article 134 offense") is neither preempted by Article 104, UCMJ, nor punishable under Article 92, UCMJ. The prosecution also requests the Court make findings as to the elements of the Article 134 offense.

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the Defense bears the burden of persuasion and must prove any factual issues necessary to decide this motion by a preponderance of the evidence. See Manual for Courts-Martial (MCM), United States, Rule for Courts-Martial (RCM) 905(c) (2008).

FACTS

The prosecution stipulates to those facts set forth in paragraphs 3-4 of Defense Motion, except for the statement that the "case has been referred to a general court martial by the convening authority with a special instruction that the case is not a capital referral." Def. Mot. at 1. The above-captioned case was referred to a general court-martial without special instructions. The prosecution further disputes any argument contained therein.

The Specification of Charge I (the "Article 104 offense") reads that the accused, "without proper authority, knowingly [gave] intelligence to the enemy, through indirect means." Enclosure 1.

The Article 134 offense reads that the accused "wrongfully and wantonly cause[d] to be published on the internet intelligence belonging to the United States government, having knowledge that intelligence published on the internet is accessible to the enemy, such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces." Enclosure 1.

U.S. Department of the Army, Pam. 27-9, Military Judges' Benchbook (1 January 2010) (Benchbook), lists the following elements for the Article 134, Uniform Code of Military Justice (UCMJ), offense relating to Specification 1 of Charge II:

APPELLATE EXHIBIT 60
PAGE REFERENCED: _____
PAGE ____ OF ____ PAGES

(1) That (state the time and place alleged), the accused (here state the act, conduct, or omission alleged); and

(2) That, under the circumstances, the conduct of the accused was (to the prejudicial of good order and discipline in the armed forces) (or) (of a nature to bring discredit upon the armed forces).

The Benchbook lists the following elements for Giving Intelligence to the Enemy under Article 104(2):

(1) That (state the time and place alleged), the accused, without proper authority, knowingly gave intelligence information to (a) certain person(s), namely: (state the name or description of the enemy alleged to have received the intelligence information);

(2) That the accused did so by (state the manner alleged);

(3) (state the name or description of the enemy alleged to have received the intelligence information) was an enemy; and

(4) That this intelligence information was true, at least in part.

WITNESSES/EVIDENCE

The prosecution does not request any witnesses be produced for this Motion. The prosecution requests that the Court consider the following enclosures to this Motion in its ruling.

1. Charge Sheet (already provided in record)
2. Government Response to Defense Bill of Particulars, 8 March 2012 (Appellate Exhibit XIV)
3. Army Regulation 380-5, Paragraph 1-21a

LEGAL AUTHORITY AND ARGUMENT

The prosecution requests that the Court deny the Defense Motion because the Article 134 offense is neither preempted by Article 104 nor punishable under Article 92.

I: THE ARTICLE 134 OFFENSE IS NOT PREEMPTED BY ARTICLE 104.

Military courts adopt a two-part test for determining whether the preemption doctrine applies. See United States v. Wright, 5 M.J. 106, 110-11 (C.M.A. 1978). The test is as follows: first, “whether Congress intended to limit prosecution for wrongful conduct within a particular area or field to offenses defined in specific articles of the Code; [and second] whether the offense charged is composed of a residuum of elements of a specific offense and asserted to be a violation of...Article 134[.]” Id., at 110-11. The preemption doctrine “requires an affirmative

answer to [both] questions.” Id., at 110. In Anderson, the Court of Appeals for the Armed Forces (CAAF) squarely answered both questions as they relate to this case in the negative. See United States v. Anderson, 68 M.J. 378, 387 (C.A.A.F. 2010).

A. The CAAF in Anderson Concluded that Congress Did Not Intend to Limit Prosecution of the Accused’s Misconduct to Article 104.

The preemption doctrine does not apply, unless “Congress intended the other punitive article to cover a class of offenses in a complete way.” United States v. Kick, 7 M.J. 82, 85 (C.M.A. 1979). Military courts “require[] Congress to indicate through direct legislative language or express legislative history that particular actions or facts are limited to the express language of an enumerated article, and may not be charged under [another punitive article].” See Anderson, 68 M.J. at 387. Military courts are “extremely reluctant to conclude that Congress intended [] provisions to preempt [an] offense...in the absence of a *clear showing* of a contrary intent.” Kick, 7 M.J. at 85 (emphasis added) (stating that there is no congressional intent to preempt offense of negligent homicide from spectrum of punishable criminal homicides); see also United States v. Erickson, 61 M.J. 230 (C.A.A.F. 2005) (“[T]he legislative history of Article 112a reflects congressional intent to not cover the class of drug-related offenses in a complete way.”); see also United States v. McGuinness, 35 M.J. 149 (C.M.A. 1992) (“[N]othing in the legislative history of Article 92 and 134 indicat[e] that Congress intended that general orders would preempt offenses made applicable to the military [under] Article 134.”). The defense argues that Congress clearly intended Article 104 to occupy the field of aiding or communicating with the enemy. This argument conflicts with the CAAF ruling in Anderson. See id., at 387.

The CAAF in Anderson concluded Article 104 did not preempt an Article 134 offense for distributing sensitive material to individuals not authorized to receive it. See id., at 386-7.¹ In Anderson, the appellant provided comprehensive information about his unit’s pending deployment to a purported Muslim extremist through a series of email communications. The purported “extremist,” a concerned American citizen, notified the Federal Bureau of Investigation (FBI) who opened an investigation and began communicating with the appellant. The appellant later provided undercover FBI agents, posing as al Qaeda operatives, computer diskettes containing classified information on the vulnerabilities of military operations. The appellant was convicted of attempting to give intelligence to the enemy, attempting to aid the enemy, and conduct prejudicial to good order and discipline. See id.

On appeal, the appellant argued that Article 104 preempted the Article 134 offense. The CAAF denied this argument, concluding that “the legislative history of Article 104 does not clearly indicate that Congress intended for offenses similar to those at issue [i.e., the distribution of sensitive material to individuals not authorized to receive it] to only be punishable under Article 104 to the exclusion of Article 134.” Id., at 387; see also UCMJ art. 104 (2008); see also

¹ In Anderson, the appellant was charged with violating, *inter alia*, Article 104, by “attempt[ing] to, without proper authority, knowingly give intelligence to the enemy, by disclosing true information to [persons] whom the [appellant] thought were Tariq Hamdi and Mohammed, members of the al Qaida terrorist network,” and Article 134, by “wrongfully and dishonorably provid[ing] information on U.S. Army troop movements...to [persons] whom the [appellant] thought were Tariq Hamdi and Mohammed, members of the al Qaida terrorist network, such conduct being prejudicial to good order and discipline in the armed forces, and of a nature to bring discredit upon the armed forces.” Anderson, 68 M.J. at 378.

UCMJ art. 134 (2008). The CAAF noted that its “reasoning could just as easily be applied to the distribution of information to individuals who are not necessarily the enemy, such as a newspaper report or...the private citizen who first encountered appellant [online].” *Id.*, at 387 (“if this distinction was not permissible...Congress was free to clearly state that Article 104 supersedes Article 134 in this context”). Here, the accused is charged with causing intelligence to be published on the internet in violation of Article 134, an offense within the reasoning of the CAAF in Anderson.

Accordingly, this Court should answer the first prong of the preemption doctrine in the negative. The Article 134 offense is not preempted by Article 104.

B. The Article 134 Offense is Not Composed of a Residuum of Elements of a Specific Offense and Asserted to be a Violation of Article 134, UCMJ.

Even assuming, *arguendo*, the Court finds that Congress intended Article 104 to preempt the conduct underlying the Article 134 offense, the preemption doctrine does not apply because the Article 134 offense is not composed of a residuum of those elements for Article 104. The prosecution respectfully requests that the Court make findings with respect to the elements of the Article 134 offense consistent with those enumerated in the Benchbook. The prosecution requests that the Court adopt the following elements to the Article 134 offense:

- (1) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 27 May 2010, cause to be published on the internet intelligence belonging to the United States government;
- (2) That the accused did so wrongfully and wantonly;
- (3) That the accused had knowledge that intelligence published on the internet is accessible to the enemy; and
- (4) That, under the circumstances, the conduct of the accused was to the prejudicial of good order and discipline in the armed forces and of a nature to bring discredit upon the armed forces.

The purpose of the preemption doctrine is to “prevent a prosecutor from circumventing an essential element of an offense under the Code.” United States v. Wagner, 52 M.J. 634, 637 (N-M. Ct. Crim. App. 1999); see also McGuinness, 35 M.J. at 152 (“the underlying basis for the preemption doctrine is Congress’ and this Court’s longstanding unwillingness to permit prosecutorial authorities ‘to eliminate vital elements from common law crimes and offenses expressly defined by Congress and permit the remaining elements to be punished as an offense under Article 134’ (citing United States v. Norris, 1953 WL 1616 (C.M.A. 1953)); but see also Erickson, 61 M.J. at 233 (“[S]imply because the offense charged under Article 134 embraces all but one element of an offense under another article does not trigger operation of the preemption doctrine.”). Here, the Article 104 offense and the Article 134 offense consist of different elements of proof, targeting distinct courses of criminal conduct.

The Article 134 offense is not composed of a residuum of elements of the Article 104 offense. First, each offense requires a different *mens rea*. See Enclosure 1. The Article 134 offense requires that the accused “wrongfully and wantonly” caused to be published on the internet intelligence belonging to the United States government.² In contrast, the Article 104 offense requires that the accused “knowingly” gave intelligence to the enemy.³ Second, the Article 134 offense requires proof that the accused caused intelligence to be published on the internet. The Article 104 offense has no such element. See United States v. Kowalski, 69 M.J. 705, 707 (C.G. Ct. Crim. App. 2010) (holding that Articles 125 and 120 are not preempted by Article 134 because those punitive articles “have an obvious additional element”); see also United States v. Tenney, 60 M.J. 838, 842 (N-M. Ct. Crim. App. 2005) (“[T]he federal bank fraud statute is not a residuum of elements of larceny, but rather, requires that the Government prove an additional element, namely, that the appellant defrauded a financial institution.”). The Government’s Response to Defense Bill of Particulars does not create this element for the Article 104 offense. See Enclosure 2; see also United States v. Fosler, 70 M.J. 225, 245 (C.A.A.F. 2011) (noting that the purpose of a bill of particulars is to provide notice to the defense). Third, the Article 134 offense requires the misconduct to be “prejudicial to good order and discipline in the armed forces and [] of a nature to bring discredit upon the armed forces.” See Enclosure 1; see also Fosler, 70 M.J. at 230 (stating that the three clauses of Article 134 are three distinct and separate parts); see also Kowalski, 69 M.J. at 707 (Articles 125 and 120 are not preempted by Article 134 because those punitive articles “have an obvious additional element”). Fourth, the Article 134 offense requires that the accused had knowledge that intelligence published on the internet is accessible to the enemy. See *id.* Fifth, the act underlying the Article 134 offense is different than the act underlying the Article 104 offense. The Article 134 offense requires the act of causing intelligence to be published on the internet, and the Article 104 offense requires the act of giving intelligence to the enemy. See Enclosure 1. Black’s Law Dictionary defines the act of giving as “to voluntarily transfer to another without compensation” and the act of causing as “to bring about or effect.” Black’s Law Dictionary (9th ed. 2009). And lastly, the Article 104 offense requires an additional element of receipt of intelligence by the enemy; the Article 134 offense does not. In sum, the charges share few, if any, elements.

As in Anderson, the Article 104 and Article 134 offenses may encompass “parallel facts” yet are “nevertheless directed at distinct conduct.” See Anderson, 68 M.J., at 387. In Anderson, “the charges were based on a single transmission of information to those appellant believed to be the enemy.” *Id.*, at 380. Here, the charges are based on a series of transmissions of information, yet are directed at distinct criminal conduct. See Enclosures 1-2; see also United States v. Canatelli, 5 M.J. 838, 841 (A.C.M.R. 1978) (noting that the preemption doctrine does not apply

² “‘Wanton’ includes ‘reckless,’ but...may, in a proper case, connote willfulness, or a disregard of probable consequences, and thus describe a more aggravated offense.” UCMJ art. 111(c)(8) (2008) (defining “wanton” under Article 111, UCMJ); see also Model Penal Code Section 2.02(2)(c) (“A person acts recklessly with respect to a material element of an offense when he consciously disregards a substantially and unjustifiable risk that the material element exists or will result from his conduct.”).

³ “A person acts knowingly with respect to a material element of an offense when: (i) if the element involves the nature of his conduct or the attendant circumstances, he is aware that his conduct is of that nature or that such circumstances exist; and (ii) if the element involves a result of his conduct, he is aware that it is practically certain that his conduct will cause such a result.” Model Penal Code Section 2.02(2)(b).

when the offenses are separate and distinct crimes). The defense argues the charges are aimed at the exact same conduct – the accused’s alleged publication of United States intelligence information on the internet. To the contrary, the Article 134 offense addresses misconduct that is distinct from the misconduct covered under the Article 104 offense. The Article 134 offense is directed to hold a Soldier criminally liable for causing intelligence to be published on the internet, with the knowledge that intelligence published on the internet is accessible to the enemy, without any requirement of the enemy being in possession of the intelligence. The Article 104 offense is directed to hold a Soldier criminally liable for knowingly giving intelligence to the enemy. See Canatelli, 5 M.J. at 841.

Accordingly, this Court should answer the second prong of the preemption doctrine in the negative. The Article 134 offense is not preempted by Article 104.

II: THE OFFENSE FOR WHICH THE ACCUSED IS CHARGED IS NOT PUNISHABLE UNDER ARTICLE 92.

In the alternative, the defense argues that the Article 134 offense must be charged as a violation of Article 92, UCMJ, in light of Army Regulation (AR) 380-5, para. 1-21a. See Enclosure 3. The defense bases its argument largely upon the Air Force Court of Criminal Appeals ruling in Borunda. See United States v. Borunda, 67 M.J. 607 (A.F. Ct. Crim. App. 2009). In Borunda, the court held that “when a lawful general order or regulation proscribing the [offense] exists, an order or regulation which by definition is punitive, the [offense], if charged, will only survive legal scrutiny as a violation of Article 92(1) and not as a violation of Article 134.” Id., at 609. Where a lawful general order or regulation does not exist, the prosecutor is “at legal liberty to charge the [accused’s offense] as a violation of Article 92(3), UCMJ, or Article 134, UCMJ[.]” Id., at 609-10. Here, no lawful general order or regulation exists that governs the specific misconduct which serves as a basis for the Article 134 offense.

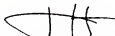
The Article 134 offense is distinct from an Article 92 offense under AR 380-5, para. 1-21a, for many reasons. See UCMJ art. 92 (2008). First, AR 380-5, para. 1-21a, subjects Department of Army personnel to sanctions, not limited to UCMJ action, if they “disclose *classified or sensitive information* to unauthorized persons.”⁴ Enclosure 3 (emphasis added). Proving information is “classified or sensitive” requires, *inter alia*, proof that the information is classified or sensitive (e.g., a classification review). On the other hand, the accused is charged with, *inter alia*, causing to be published on the internet “*intelligence* belonging to the United States.” Enclosure 1 (emphasis added). Intelligence is not limited only to classified or sensitive information. Accordingly, such misconduct falls outside the generalized misconduct proscribed under AR 380-5, para. 1-21a. Second, the *mens rea* under the Article 134 offense and AR 380-5 are different. The Article 134 offense requires that the accused acted “wrongfully and wantonly.” Enclosure 1. AR 380-5, para. 1-21a, subjects Department of Army personnel to sanctions if they commit misconduct “knowingly, willfully, or negligently.” Enclosure 3. Lastly, the Article 134 offense, as written, requires that the accused had “knowledge that intelligence published on the internet is accessible to the enemy.” Enclosure 1.

⁴ Sanctions are not limited to UCMJ action, but also can include, without limitation, warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and removal of original classification authority. See Enclosure 3.

In sum, the Article 134 offense captures more than classified or sensitive information and requires additional elements and a different *mens rea* than an Article 92 offense under AR 380-5, para. 1-21a. Accordingly, the prosecution is "at legal liberty to charge the [accused's offense] as a violation of Article 92(3), UCMJ, or Article 134[.]" Borunda, 67 M.J. at 609-10.

CONCLUSION

Based on the above, the prosecution requests that the Court deny Defense Motion to Dismiss Specification 1 of Charge II for Failure to State an Offense because the Article 134 offense is neither preempted by Article 104 nor punishable under Article 92.



J. HUNTER WHYTE
CPT, JA
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 12 April 2012.



J. HUNTER WHYTE
CPT, JA
Assistant Trial Counsel

Appellate Exhibit 60
Enclosure 1
is the charge sheet

Appellate Exhibit 60
Enclosure 2
has been entered into the
record as
Appellate Exhibit 14

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Prosecution Response to

Defense Motion to Dismiss Specification 1
of Charge II for Failure to
State an Offense

Enclosure 3

12 April 2012

Security

Department of the Army Information Security Program

Headquarters
Department of the Army
Washington, DC
29 September 2000

UNCLASSIFIED

have confidence in the sharing of information with other agencies, the national, DOD, and DA policy, contained in this regulation, will be followed.

b. Unless otherwise noted, requests for waivers to the requirements contained in this regulation, will be submitted, through command channels, to DAMI-CH. Waivers to DOD requirements will be forwarded by DAMI-CH, for decision to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)). For requirements related to Two-Person Integrity (TPI), RD, Foreign Government Information (FGI) (including North Atlantic Treaty Organization (NATO)), and security arrangements for international programs, waivers will be forwarded to the Under Secretary of Defense (Policy)(USD(P)). Waivers for SAPs will be submitted, through SAPs channels, to DAMI-CH for coordination with TMO and, as required, forwarded to the Under Secretary of Defense (Special Programs) (USD(SP)). The ASD(C3I) and USD(P) are responsible for notifying the Director of the ISOO of the waivers approved that involve EO 12958 and its implementing directives.

c. Before submitting a request for waiver, the requesting authority will consider risk management factors such as criticality, sensitivity, and value of the information, analysis of the threats both known and anticipated, vulnerability to exploitation, and countermeasure benefits versus cost (national security cost and resource cost). Requests for waiver must contain sufficient information to permit a complete and thorough analysis to be made of the impact on national security if the waiver is approved. The waiver request will also describe all the factors creating the special situation and the alternative or compensatory measures which make sure the protection afforded the information is sufficient to reasonably deter and detect loss or unauthorized disclosure. The requesting command will maintain documentation regarding approved waivers, including the alternative or compensatory measures approved and in use, and furnish this documentation, upon request, to other agencies and to other Army commands, with whom classified information or secure facilities are shared.

Note: Waivers granted before the effective date of this regulation are canceled no later than one year after the effective date of this regulation. New/updated waiver requests may be submitted prior to cancellation date.

d. Throughout this regulation there are references to policy subject to MACOM approval or subject to policy as the MACOM directs. Where that language, in substance, is used, the MACOM commander, or the HQDA SAAA, for cases involving HQDA and its Field Operating Agencies (FOA), can delegate such approval authority. The delegations will be in writing. A copy of such delegations will be maintained by the appointing official and reviewed periodically for review of need for continuation. Where this regulation specifically specifies waiver authority to a MACOM commander or the HQDA SAAA, that authority resides solely with the MACOM commander or HQDA SAAA and will not be further delegated.

Section VII

Corrective Actions and Sanctions

1-20. General

Commanders will establish procedures to make sure that prompt and appropriate action is taken concerning a violation of the provisions of this regulation, especially in those cases involving incidents which can put classified information at risk of compromise, unauthorized disclosure, or improper classification of information. Such actions will focus on a correction or elimination of the conditions that caused or contributed to the incident.

1-21. Sanctions

a. DA personnel will be subject to sanctions if they knowingly, willfully, or negligently—

- (1) Disclose classified or sensitive information to unauthorized persons.
- (2) Classify or continue the classification of information in violation of this regulation.
- (3) Violate any other provision of this regulation.

b. Sanctions can include, but are not limited to warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and removal of original classification authority. Action can also be taken under the Uniform Code of Military Justice (UCMJ) for violations of that Code and under applicable criminal law, if warranted.

c. Original classification authority will be withdrawn from individuals who demonstrate a disregard or pattern of error in applying the classification and sensitivity standards of this regulation.

1-22. Reporting of Incidents

EO 12958, paragraph 5.7(e)(2), requires that the director of the ISOO be advised of instances in which classified information is knowingly, willfully, or negligently disclosed to unauthorized persons, or instances of classifying, or continuing the classification of, information in violation of this regulation. Reports of those instances will be submitted through command channels to DAMI-CH for forwarding to the director of the ISOO and other defense officials as appropriate. See chapter 10 for reporting of other security incidents.

13 April 2012

MEMORANDUM FOR RECORD

SUBJECT: Detailed Military Counsel

1. I have thoroughly discussed my options regarding my detailed military counsel with Mr. Coombs. We have spoken about the advantages and disadvantages of retaining my detailed counsel, MAJ Matthew Kemkes and CPT Paul Bouchard, on my case.
2. I elect to excuse my detailed counsel MAJ Kemkes and CPT Bouchard. I request that CPT Joshua Tooman be detailed to my case as my military counsel. I do not request any other defense counsel to be detailed to my case at this time.



BRADLEY MANNING
PFC, U.S. Army

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army, xxx-xx-)

Headquarters and Headquarters Company, U.S.)

Army Garrison, Joint Base Myer-Henderson Hall,)

Fort Myer, VA 22211)

**DEFENSE MOTION TO
DISMISS THE SPECIFICATION
OF CHARGE I FOR FAILURE
TO STATE AN OFFENSE**

DATED: 29 March 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, pursuant to applicable case law, Rule for Courts Martial (R.C.M.) 907(b)(1)(B), and the First and the Fifth Amendments to the United States Constitution, requests this Court to either dismiss the Specification of Charge I for failing to state an offense or determine that the term "indirectly," as used in Article 104, is unconstitutionally vague in violation of the First and Fifth Amendments and renders Article 104 substantially overbroad in violation of the First Amendment to the United States Constitution.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. The Defense, as the moving party, bears the burden of this motion by a preponderance of the evidence pursuant to R.C.M. 905(c)(1) and (2).

FACTS

3. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of conduct prejudicial to good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting government property, and two specifications of knowingly exceeding authorized access to a government computer, in violation of Articles 92, 104, and 134, Uniform Code of Military Justice (UCMJ) 10 U.S.C. §§ 892, 904, 934 (2010). The case has been referred to a general court martial by the convening authority with a special instruction that the case is not a capital referral.

4. In the Specification of Charge I, the Government pleads that PFC Manning “between on or about 1 November 2009 and on or about 27 May 2010, without proper authority knowingly gave intelligence to the enemy, through indirect means.” On 14 February, 2012, the Defense pursuant to R.C.M. 906 moved this Court to direct the Government to respond to a bill of particulars in the subject case on the grounds that it was necessary for PFC Manning to understand the charges against him so that he could adequately prepare his defense and not be subject to unfair surprise at trial. The Defense asked in its particulars, “How did PFC Manning knowingly give intelligence to the enemy?” The Government’s response was that PFC Manning knowingly gave intelligence to the enemy by “transmitting certain intelligence, specified in a separate classified document, to the enemy through the WikiLeaks website.” See Government Bill of Particulars. The Government’s theory of how PFC Manning knowingly gave information to the enemy fails to allege the requisite intent within the meaning of Article 104 and, as such, the Specification and Charge should be dismissed for failure to state an offense. In the alternative, the Defense argues that Article 104, as applied in this case, violates the Due Process and First Amendment rights of PFC Manning.

WITNESSES/EVIDENCE

5. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this court to consider the following evidence in support of the Defense’s motion.

- a. Chat Logs Excerpt;
- b. Charge Sheet;
- c. Continuation of DD Form 457.

LEGAL AUTHORITY AND ARGUMENT

A. The Government Fails to State an Offense Because It Has Failed to Allege the Requisite Intent Under Article 104

6. The Government fails to state an offense under Article 104 because it has not alleged the requisite intent. Every court interpreting Article 104(2) has held that the Government must prove general criminal intent to give intelligence to, or communicate with, the enemy; indeed, no prosecution under this Article has ever been maintained without some allegation of *mens rea*. Additionally, if the Government’s interpretation of “indirectly” is to be accepted, a staggering amount of conduct would be punishable under Article 104. Accordingly, the Government’s interpretation of “indirectly” is untenable because it does not require a showing of the requisite criminal intent.

7. Article 104 punishes “[a]ny person who – (1) aids, or attempts to aid, the enemy with arms, ammunition, supplies, money, or other things; or (2) without proper authority, knowingly harbors or protects or gives intelligence to, or communicates or corresponds with or holds any intercourse with the enemy, either directly or indirectly.” 10 U.S.C. § 904. The Government’s theory – that PFC Manning indirectly aided the enemy because he knowingly caused to be published on the internet United States intelligence with the knowledge that such intelligence would be accessible to the enemy – does not state an offense because it does not allege that PFC Manning acted with the requisite intent.¹

8. Courts have uniformly held that the Government must allege and prove a general criminal intent to give intelligence to, or communicate with, the enemy under Article 104(2). See *United States v. Anderson*, 68 M.J. 378, 387 (C.A.A.F. 2010); *United States v. Batchelor*, 22 C.M.R. 144, 157 (C.M.A. 1956) (expressing “no doubt” that Article 104, which “is so closely akin to treason” requires a “showing of criminal intent”); *United States v. Olson*, 20 C.M.R. 461, 464 (A.B.R. 1955). In fact, no prosecution under Article 104(2) has been maintained without an allegation that the accused intended to give intelligence to, or communicate with, the enemy in some way.

9. In *Olson*, for example, the accused was a prisoner of war convicted under Article 104 for aiding the enemy by making speeches and writing publications favorable to his captors and unfavorable to the United States. 20 C.M.R. at 462. In affirming the conviction, the United States Army Board of Review held that Article 104 “does require a general evil intent in order to protect the innocent who may commit some act in aiding the enemy inadvertently, accidentally, or negligently.” *Id.* at 464. The court found the accused’s conduct to evidence this requisite general “evil intent.” *Id.*

10. Similarly, the Court of Military Appeals in *Batchelor* held that a prosecution under Article 104 requires a showing of general intent to aid the enemy. 22 C.M.R. at 157. The accused in *Batchelor* was also a prisoner of war who made several speeches and public broadcasts within his prison camp that criticized and condemned the United States. *Id.* at 150. The accused also directly gave information regarding fellow prisoners of war to his captors. *Id.* at 150-51. In affirming his conviction, the court highlighted the significance of the accused’s direct participation with an enemy of the United States by approving of the law officer’s instructions on the elements of Article 104:

He [the law judge] informed the court-martial members that a verdict of guilty could not be returned unless they were satisfied beyond a reasonable doubt that the accused, without proper authority, had

¹ The Government has proceeded under the “gives intelligence to . . . the enemy, either directly or indirectly” clause of Article 104(2). 10 U.S.C. § 904(2). It has not proceeded specifically under the theory that PFC Manning improperly “communicat[ed]” with the enemy. However, if the Government’s interpretation of the term “indirectly” is accepted, that interpretation will apply equally to the clause prohibiting communication, thereby sweeping in an enormous amount of constitutionally protected speech.

knowingly participated with the Chinese Communists in planning a subversive organization, had knowingly conducted study groups, made speeches, drafted and circulated “peace” petitions, and expounded Communist propaganda viewpoints, and *that he knew at the time that the people he was collaborating with were enemies of the United States*. The law officer then characterized these offenses as requiring a general criminal intent and instructed on honest belief as a defense.

Id. at 156 (emphases supplied). The court also approved the law officer’s instructions on the term “knowingly:”

“Specifications 1 and 2 of Charge I allege ‘knowingly communicated, corresponded, and held intercourse with the enemy.’ You are advised that by ‘knowingly,’ as used in Specification 1 and Specification 2 of Charge I is meant *that accused knew he was dealing with an enemy of the United States* and that he had full knowledge of all the facts alleged in the specification after the word ‘knowingly.’”

Id. at 156-57 (emphasis supplied) (quoting law officer’s instructions). The court emphasized that “[w]e have no doubt that [defense] counsel are on sound ground when they assert that [Article 104] requires a showing of criminal intent, and the Government concedes that premise to be true . . . [S]urely an offense which is so closely akin to treason and may be punished by a death sentence cannot be viewed as a ‘public welfare’ kind of dereliction.” *Id.* at 157. The court concluded that “the law officer’s instructions, requiring as they did the finding of general criminal intent and a finding as to words importing criminality, were correct.” *Id.* at 158. Therefore, the accused’s knowledge that he was dealing with the enemy was central to finding the general criminal intent to aid the enemy, an essential element of an Article 104 prosecution.

11. Along the same lines, the Court of Appeals for the Armed Forces in *Anderson* demonstrated the necessity of a general criminal intent to aid the enemy in an Article 104 charge. The accused in *Anderson* was convicted of attempting to provide sensitive intelligence information to the enemy. 68 M.J. at 380. Specifically, the accused provided emails including “comprehensive information about the number of soldiers in his unit, their training programs, and the precise location to which his unit would be deploying” to a person he believed to be a “Muslim extremist,” who in reality was a concerned American citizen attempting to thwart terrorist activities. *Id.* at 381. The accused also met with undercover FBI agents whom he believed to be Al Qaeda operatives and disclosed to them “computer diskettes containing classified information on the vulnerabilities of various military vehicles, the vulnerabilities of his unit as they travelled to Iraq, and other sensitive information.” *Id.* The *Anderson* Court highlighted the need for a general criminal intent under Article 104 by contrasting Article 104 with the more general Article 134:

[W]hile the two charges in this case have parallel facts, as charged they are nonetheless directed at distinct conduct. The Article 104, UCMJ, charge was directed at [Anderson's] attempt to aid the enemy directly. The Article 134, UCMJ, charge was directed towards the distribution of sensitive material to individuals not authorized to receive it in this case Criminal Investigation Command agents posing as the enemy, but the reasoning could just as easily be applied to the distribution of information to individuals who are not necessarily the enemy, such as a newspaper reporter, or for that matter the private citizen who first encountered [Anderson] on the "Brave Muslim" website. *Unlike Article 104, UCMJ, the general offense as charged prohibits the dissemination of the information regardless of the intent behind that dissemination.* If this distinction was not permissible in light of Article 104, UCMJ, Congress was free to clearly state that Article 104, UCMJ, supersedes Article 134, UCMJ, in this context.

Id. at 387 (emphasis supplied). Thus, *Anderson* makes clear that Article 104(2) requires the Government to allege that the accused intended to directly or indirectly provide intelligence to, or communicate with, the enemy; mere dissemination of information to persons unauthorized to receive it is insufficient without the necessary criminal intent. *See id.*; *Olson*, 20 C.M.R. at 464.

12. Finally, the general criminal intent to aid the enemy was readily apparent in several other Article 104 cases where the court did not specifically address the issue of requisite intent under Article 104. In *United States v. Sombolay*, for example, the accused sold U.S. intelligence information to an undercover U.S. intelligence agent posing as a representative of the Jordanian government. 37 M.J. 647, 648 (A.C.M.R. 1993). The accused had also previously sold intelligence information to representatives of Iraq. *Id.* Similarly, in *United States v. Garwood*, the accused, a prisoner of war in a Vietnamese prison camp, informed against his fellow prisoners and helped the captors lead political indoctrination discussions among the prisoners. 16 M.J. 863, 867 (N-M.C.M.R. 1983), *aff'd*, 20 M.J. 148 (C.M.A. 1985). Likewise, the accused in *United States v. Johnson* admitted to attempting to contact the Viet Cong on two separate instances of unauthorized absence. 43 C.M.R. 160, 161 (C.M.A. 1971). Along the same lines, in *United States v. Dickenson*, the accused, a prisoner of war in a Chinese prison camp in Korea, wrote petitions and made speeches favorable to the Chinese Communists and unfavorable to the United States and also informed against fellow prisoners. 20 C.M.R. 154, 171 (C.M.A. 1955). In each of these cases, the requisite general criminal intent to provide intelligence to, or communicate with, the enemy was evident from each accused's conduct.

13. It is clear that in order to state an offense under Article 104(2), the Government must allege that PFC Manning intended to "give[] intelligence to . . . the enemy" and that PFC Manning did so through indirect means. The intent required is the intent to give the

intelligence to the enemy. For instance, if PFC Manning had printed intelligence information and contacted FedEx to deliver the information to the enemy, he would presumably be guilty of “giv[ing] intelligence . . . to the enemy” indirectly. The term “indirectly” punishes conduct where an accused employs a third party intermediary *for the purpose of* “giv[ing] intelligence to . . . the enemy.” The term “indirectly” is not intended to capture the scenario where an accused’s disclosure to a third party has the eventual result of intelligence information being accessible to the enemy.

14. Intending to “give[] intelligence to . . . the enemy” and knowing that, if intelligence information is improperly disclosed, it may potentially be accessible to the enemy are two very different things. The former criminalizes an act with a guilty mind – the intent of the accused to “give[] intelligence to . . . the enemy.” The latter, on the other hand, criminalizes the inadvertent, accidental, or negligent conduct that Article 104(2) is clearly not intended to reach. *See Olson*, 20 C.M.R. at 464. To hold that negligent conduct in disclosing intelligence information, devoid of an intent to actually “give[] intelligence . . . to the enemy,” is actionable under Article 104 is to turn a crime that carries with it the possibility of the death penalty into a strict liability offense. Such an interpretation is not tenable.

15. The interpretation of Article 104(2) as requiring intent to give intelligence to the enemy is further supported by the Military Judges’ Benchbook. In the Model Specification to 104(2) (“Giving Intelligence to the Enemy”), the Military Judges’ Benchbook provides:

b. MODEL SPECIFICATION:

In that _____ (personal jurisdiction data) did, (at/on board—
location), on or about _____, without proper authority, *knowingly*
give intelligence to the enemy (by informing a patrol of the enemy’s
forces of the whereabouts of a military patrol of the United States forces)
(_____).

Dept. of the Army, Pamphlet 27-9, Legal Services, Military Judges’ Benchbook, para. 3-28-4 (1 Jan. 2010) [hereinafter Benchbook] (emphasis supplied). The term “knowingly” means that the accused had to intend to give the intelligence to the enemy, not that the accused knew that, by giving it to a third party, it might eventually end up in the hands of the enemy.

16. Although the Model Specification for “Giving Intelligence to the Enemy” does not contain any specific information about doing so through indirect means, the Model Specification for “Communicating with the Enemy”² does:

² Giving intelligence to the enemy is a particularized form of communicating with the enemy; thus, the Model Specifications for communicating with the enemy are also broadly applicable to giving intelligence to the enemy.

b. MODEL SPECIFICATION:

In that _____ (personal jurisdiction data) did, (at/on board—location), on or about _____, without proper authority, knowingly (communicate with) (correspond with) (hold intercourse with) the enemy (by writing and transmitting secretly through lines to one _____ whom he/she, the accused, knew to be (an officer of the enemy's armed forces) (_____)) a communication in words and figures substantially as follows, to wit: (_____ (indirectly by publishing in _____, a newspaper published at _____, a communication in words and figures as follows, to wit: _____, which communication was intended to reach the enemy) (_____)).

Id. para. 3-28-5. The Model Specification contemplates specifically the scenario where “a newspaper” is the method by which the accused indirectly communicated with the enemy. Under the Model Specification, the communication via the newspaper intermediary must have been “intended to reach the enemy.” *Id.* Where the accused did not intend to reach the enemy – even if the accused knew that the information or communication published by the newspaper could potentially be accessible to the enemy – an offense cannot be stated under Article 104(2).

17. The Government has not properly alleged that PFC Manning indirectly gave intelligence to the enemy under Article 104(2). The Government has not alleged that PFC Manning intended to give intelligence to, or communicate with, the enemy in making the alleged disclosure to WikiLeaks. Rather, the Government has merely alleged that PFC Manning had knowledge that the information, *if* ultimately published, *might* be accessible to the enemy and that such information *might* help the enemy. Such a feeble *mens rea* allegation is patently insufficient to establish the requisite intent under Article 104.

18. Not only has the Government failed to adduce any evidence that PFC Manning intended to give intelligence to the enemy through indirect means, but there is evidence suggesting the opposite – that PFC did not intend to give intelligence to the enemy. In the purported chat logs between PFC Manning and government informant Adrian Lamo, Lamo allegedly asked PFC Manning why he did not sell the information to a foreign government and “get rich off it[.]” In response, PFC Manning expressly disclaimed any intent to help any enemy of the United States:

[B]ecause it's public data . . . it belongs in the public domain . . . information should be free . . . it belongs in the public domain . . . *because another state would just take advantage of the information . . . try and get some edge . . . if it's out in the open . . . it should be a public good.*

See Attachment A (Chat Logs between PFC Bradley Manning and Adrian Lamo (last visited on 22 March 2012), available at <http://www.wired.com/threatlevel/2011/07/>

manning-lamo-logs/ (emphasis supplied)). Far from intending to aid any enemy of the United States, PFC Manning's actions and statements illustrate a conscious rejection of any such ill motive. Indeed, PFC Manning refused to sell the information to another country, even though he could have financially benefitted by doing so, because he did *not* want an enemy of the United States to "take advantage of the information[.]" *Id.* The chat logs show that since PFC Manning did not intend to aid the enemy, he surely did not intend to give intelligence information to the enemy. In this respect, PFC Manning's alleged conduct and statements stand in stark contrast to the conduct of the accused in *Anderson*, who actively attempted to directly give sensitive information to Al Qaeda operatives in an effort to sabotage American operations abroad. *See Anderson*, 68 M.J. at 381.

19. Thus, because the Government has not alleged that PFC Manning acted with the requisite intent to give intelligence to, or communicate with, the enemy, the Government does not state a cognizable Article 104 offense against PFC Manning. Accordingly, this Specification and Charge should be dismissed.

B. The Government's Interpretation of Article 104, as Applied in This Case, Renders Article 104 Unconstitutionally Vague Under the Fifth Amendment to the United States Constitution

20. In the alternative, the Defense submits that an expansive reading of "indirectly," as applied in this case, renders Article 104 unconstitutionally vague in violation of the Due Process Clause of the Fifth Amendment. If Article 104 is interpreted to reach PFC Manning's alleged conduct, it would be constitutionally defective because it would fail to provide sufficient notice of what conduct is prohibited and would fail to provide sufficient guidelines to govern law enforcement.

21. As a general rule, "the void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." *Kolender v. Lawson*, 461 U.S. 352, 357 (1983). The proper inquiry in a vagueness challenge to an Article of the UCMJ is whether the challenged Article provides sufficient warning for particular accuseds to reasonably understand that their specific conduct was included within the challenged Article's prohibition. *See Parker v. Levy*, 417 U.S. 733, 756-57 (1974); *United States v. Nat'l Dairy Prods. Corp.*, 372 U.S. 29, 32-33 (1963); *United States v. Brown*, 45 M.J. 389, 394 (C.A.A.F. 1996); *United States v. Johanns*, 20 M.J. 155, 158, 161 (C.M.A. 1985); *United States v. Hecker*, 42 M.J. 640, 642-43 (A.F. Ct. Crim. App. 1995) (adding that "[a] penal regulation must be definite and certain, strictly construed, and any doubt with respect to it must be resolved in favor of the accused.") (alterations and quotations omitted). The Supreme Court has pointed out that while both actual notice to the citizenry and arbitrary enforcement are prime concerns of the doctrine, the more important requirement is "the

requirement that a legislature establish minimal guidelines to govern law enforcement.”
Kolender, 461 U.S. at 357-58 (quoting *Smith v. Goguen*, 415 U.S. 566, 574 (1974)).

22. The phrase “indirectly” in Article 104, as interpreted by the Government, is unconstitutionally vague under the Due Process Clause of the Fifth Amendment because it would not provide sufficient notice of the proscribed conduct and would fail to establish any guidelines to govern law enforcement.

23. If the Government’s interpretation of Article 104 is accepted, Article 104 would be alarming in scope. Under the Government’s interpretation, no criminal intent is required; disclosure of information with the mere knowledge that the information disclosed *might* be accessible to the enemy is punishable under Article 104. The amount of conduct that is made subject to potential capital punishment under such an interpretation is staggering. For example, a top military official discussing what could broadly be classified as intelligence information with a reporter would be potentially liable under Article 104, as the official would likely have known that the information could be accessed by the enemy once the reporter publishes it. Similarly, disclosure of information regarding insufficiency of soldiers’ weapons, low morale among soldiers in a particular unit, or the prevalence of Post Traumatic Stress Disorder or suicide among servicemembers would all be subject to Article 104’s prohibition of “indirectly” providing intelligence information to, or communicating with, the enemy under the Government’s approach. In each instance, the servicemember responsible for the disclosure would be subject to a capital offense notwithstanding the absence of any intent whatsoever to provide intelligence information to, or communicate with, the enemy.

24. PFC Manning could not have reasonably concluded that causing intelligence information to be published on the internet would constitute “indirectly” giving intelligence to, or communicating with, the enemy under Article 104. Similarly, a servicemember speaking with a reporter about high suicide rates in the Army or about the prevalence of Post Traumatic Stress Disorder among servicemembers would certainly not consider this conduct as aiding or communicating with the enemy in any way. To surprise such an individual with criminal liability under Article 104 clearly offends the Due Process Clause of the Fifth Amendment.

25. The potential for liability is endless. What if a soldier sends an email to a family member that contains intelligence information and that family member, in turn, publishes that information publicly (perhaps on a blog or in an editorial piece)? Has the soldier “aided the enemy” because he indirectly communicated intelligence information to the enemy? Does the inquiry turn on whether it was foreseeable that the family member would disclose the information? Does the inquiry turn on how visible the public disclosure is? Further, how many links in the chain of “indirectly” could render the soldier subject to the death penalty? What if the family member forwards the email to a friend who, in turn, publishes it? Is the soldier guilty of aiding the enemy? The point is

that constitutional infirmities abound where “indirectly” is interpreted as the Government suggests.

26. Moreover, interpreting the phrase “indirectly” in such an expansive manner would provide virtually no guidelines to govern law enforcement. Under this definition of “indirectly,” any time a person subject to the UCMJ places *any* information on the internet that *might* be accessed by an enemy of the United States, that person will be subject to criminal liability, including the prospect of capital punishment. See 10 U.S.C. § 904 (providing for capital punishment, among other punishments). The danger of arbitrary and discriminatory enforcement under such an extension of Article 104 is readily apparent: as a staggering amount of conduct would be punishable under Article 104, law enforcement personnel will, in light of scarce resources, need to be very selective in determining which individuals to prosecute. Such a scenario opens the door for widespread arbitrary and discriminatory enforcement.

27. Therefore, as the Government’s interpretation of the term “indirectly” would fail to give sufficient guidelines to law enforcement and would also fail to give reasonable notice of what conduct Article 104 proscribes, this Court should determine that such an interpretation renders Article 104 unconstitutionally vague under the Due Process Clause of the Fifth Amendment.

C. The Government’s Interpretation of Article 104 Renders Article 104 Substantially Overbroad in Violation of the First Amendment to the United States Constitution

28. In the alternative, the Defense submits that the Government’s expansive interpretation of Article 104 renders it substantially overbroad in violation of the First Amendment. As interpreted by the Government, Article 104 would prohibit a substantial amount of constitutionally protected speech. Furthermore, this substantial overbreadth cannot be cured by assurances of prosecutorial restraint.

29. A law may be struck down on overbreadth grounds where “a substantial number of its applications are unconstitutional, judged in relation to the statute’s plainly legitimate sweep.” *United States v. Stevens*, ___ U.S. ___, 130 S.Ct. 1577, 1587 (2010) (quoting *Washington State Grange v. Washington State Republican Party*, 522 U.S. 442, 449 n.6 (2008)); see *City of Houston v. Hill*, 482 U.S. 451, 466-67 (1987).³

³ As is the case with vagueness challenges, military context matters in an overbreadth inquiry. See *Parker*, 417 U.S. at 758. In *Parker*, the Supreme Court rejected an overbreadth challenge to Articles 133 and 134 of the UCMJ because, “[w]hile there may lurk at the fringes of the articles . . . some possibility that conduct which would be ultimately held to be protected by the First Amendment could be included within their prohibition,” the Court determined that “[t]here is a wide range of the conduct of military personnel to which Arts. 133 and 134 may be applied without infringement of the First Amendment.” *Id.* at 760-61. No such determination could be made with respect to the Government’s interpretation of Article 104 however,

30. Under the Government's interpretation, Article 104 establishes "a criminal prohibition of alarming breadth." *Stevens*, 130 S.Ct. at 1588. Article 104 is substantially overbroad because, if the term "indirectly" is given the interpretation that the Government puts forth, a substantial amount of constitutionally protected speech would fall victim to Article 104's sweeping prohibition. Article 104 categorically prohibits any unauthorized communication with an enemy, regardless of whether the communication contains any intelligence information. As a result, if liability exists for issuing a communication that is not aimed at an enemy but may be indirectly accessed by the enemy, anyone subject to the UCMJ would be unable to make any public statement on any subject without fear of exposure to a capital prosecution. A person subject to the UCMJ could not speak with a newspaper reporter, for example, because the knowledge that the enemy has access to newspapers and might eventually read the reporter's article could transform any communication with the press into a prohibited correspondence with the enemy and a potentially capital crime.

31. Likewise, Article 104, as interpreted by the Government, could conceivably reach any information placed on the internet that might be accessed by the enemy, irrespective of the reason that the information was placed on the public domain in the first place and regardless of whether the information would aid the enemy in any way. So long as the person knows that the information can be potentially accessed by the enemy, the provisions of Article 104 would apply. Such a broad interpretation of Article 104 impermissibly proscribes a substantial amount of constitutionally protected speech. So interpreted, Article 104 would sweep much more broadly and carry much heavier consequences than any previous restriction on soldier speech upheld by the Court. As the impermissible applications of Article 104, as construed by the Government, "far outnumber any permissible ones[.]" it is substantially overbroad in violation of the First Amendment.⁴ *Stevens*, 130 S.Ct. at 1592.

32. Moreover, assurances of prosecutorial restraint are insufficient to cure unconstitutional overbreadth. As the Court explained in *Stevens*, "[t]he Government's assurance that it will apply [the statute] far more restrictively than its language provides is pertinent only as an implicit acknowledgement of the potential constitutional problems with a more natural reading." 130 S.Ct. at 1591. Indeed, "[t]he opportunity for abuse,

as any public statement would subject the speaker to prosecution if the enemy could conceivably access it in some form. Thus, even if there is some conduct to which Article 104 may be constitutionally applied, there is an astonishingly wide range of speech protected by the First Amendment that would subject the speaker to prosecution under the Government's interpretation of Article 104.

⁴ Even if the Government's expansive interpretation of Article 104 could somehow be limited so as to reach only information that could potentially aid the enemy without also reaching indirect communications with the enemy (a limitation that finds absolutely no support in the text of Article 104 or in the case law interpreting it), it would still render Article 104 substantially overbroad. Public statements regarding low morale among a particular unit or high rates of PTSD among servicemembers, for example, which might later be accessed by the enemy in some form can be construed as potentially aiding the enemy. Thus, under the Government's interpretation, Article 104's fatal overbreadth cannot be avoided.

especially where a statute has received a virtually open-ended interpretation, is self-evident." *Hill*, 482 U.S. at 466.

33. Therefore, if the Government's interpretation of "indirectly" is correct, this Court should determine that Article 104 is substantially overbroad in violation of the First Amendment.

CONCLUSION

34. Wherefore, in light of the foregoing, the Defense requests this Court either dismiss the Specification of Charge I for failing to state an offense or determine that the term "indirectly," as used in Article 104, is unconstitutionally vague in violation of the First and Fifth Amendments and renders Article 104 substantially overbroad in violation of the First Amendment to the United States Constitution.

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

ATTACHMENT A

Alleged Adrian Lamo – PFC Bradley Manning Chat Log

(02:22:47 PM) bradass87: i mean what if i were someone more malicious

(02:23:25 PM) bradass87: i could've sold to russia or china, and made bank?

(02:23:36 PM) info@adrianlamo.com: why didn't you?

(02:23:58 PM) bradass87: because it's public data

(02:24:15 PM) info@adrianlamo.com: i mean, the cables

(02:24:46 PM) bradass87: it belongs in the public domain

(02:25:15 PM) bradass87: information should be free

(02:25:39 PM) bradass87: it belongs in the public domain

(02:26:18 PM) bradass87: because another state would just take advantage of the information...
try and get some edge

(02:26:55 PM) bradass87: if its out in the open... it should be a public good

Later excerpt

(04:45:20 PM) info@adrianlamo.com: or a spy :)

(04:45:48 PM) bradass87: i couldn't be a spy...

(04:45:59 PM) bradass87: spies dont post things up for the world to see

27 March 2012

MEMORANDUM FOR RECORD

SUBJECT: Security Expert Review of Defense Motions

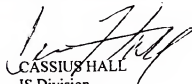
1. I hereby certify that I have reviewed the following Defense motions for the presence of classified information:

- a) Defense Motion to Dismiss the Specification of Charge I for Failure to State an Offense;
- b) Defense Motion to Dismiss Specification 1 of Charge II for Failure to State an Offense;
- and
- c) Defense Motion to Dismiss Based Upon Unreasonable Multiplication of Charges

I do not believe that any of these motions contain classified information or information that a reasonable person could believe to be classified.

2. The Unreasonable Multiplication of Charges motion does cite to classified attachments. However, these attachments will be provided separately from the motion.

3. The point of contact for this memorandum is the undersigned at [703-428-430].


CASSIUS HALL
IS Division
INSCOM G2

28 March 2012

MEMORANDUM FOR RECORD

SUBJECT: Security Expert Review of Defense Motion

1. I hereby certify that I have reviewed the following Defense motion for the presence of classified information:

a) Defense Motion to Dismiss [793 v3]

I do not believe that this motion contains classified information or information that a reasonable person could believe to be classified.

2. The point of contact for this memorandum is the undersigned at [703-428-4340].



CASSIUS HALL
IS Division
INSCOM G2

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

GOVERNMENT RESPONSE
TO DEFENSE MOTION TO
DISMISS THE SPECIFICATION
OF CHARGE I FOR FAILURE
TO STATE AN OFFENSE

12 April 2012

RELIEF SOUGHT

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny the defense motion to dismiss the Specification of Charge I for failure to state an offense. The United States also requests this Court deny the defense request to declare the term "indirectly," as used in Article 104, Uniform Code of Military Justice (UCMJ), unconstitutionally vague in violation of the First and Fifth Amendments to the United States Constitution, or substantially overbroad in violation of the First Amendment to the United States Constitution. Finally, the United States respectfully requests this Court adopt the U.S. Department of the Army, Pam. 27-9, *Military Judges' Benchbook* (1 January 2010) (*Benchbook*), elements for the offense of Giving Intelligence to the Enemy under Article 104, UCMJ.

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the defense has the burden of persuasion on any factual issue the resolution of which is necessary to decide the motion. *Manual for Courts-Martial (MCM)*, United States, Rule for Courts-Martial (RCM) 905(c)(2) (2008). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

FACTS

The United States stipulates to the facts as set forth in the defense motion, except for the following "facts" in paragraph 4:

"The Government's theory of how PFC Manning knowingly gave information to the enemy fails to allege the requisite intent within the meaning of Article 104 and, as such, the Specification and Charge should be dismissed for failure to state an offense. In the alternative, the Defense argues that Article 104, as applied in this case, violates the Due Process and First Amendment rights of PFC Manning."

Def. Mot. at 2. The United States also disputes the following statement in paragraph 3 of the Defense Motion: "The case has been referred to a general court-martial by the convening

authority with a special instruction that the case is not a capital referral.” The above-captioned case was referred to a general court-martial without special instructions.

The United States adds the following additional facts:

The *Benchbook* publishes the following model specification for Giving Intelligence to the Enemy under Article 104(2), UCMJ:

In that _____ (personal jurisdiction data) did, (at/on board—location), on or about _____, without proper authority, knowingly give intelligence to the enemy (by informing a patrol of the enemy’s forces of the whereabouts of a military patrol of the United States forces) (_____).

The *Benchbook* lists the following elements for Giving Intelligence to the Enemy under Article 104(2), UCMJ:

- (1) That (state the time and place alleged), the accused, without proper authority, knowingly gave intelligence information to (a) certain person(s), namely: (state the name or description of the enemy alleged to have received the intelligence information);
- (2) That the accused did so by (state the manner alleged);
- (3) (state the name or description of the enemy alleged to have received the intelligence information) was an enemy; and
- (4) That this intelligence information was true, at least in part.

WITNESSES/EVIDENCE

The United States requests this Court consider the following enclosures:

1. *Department of the Army, Pam. 27-9, Military Judges’ Benchbook*, Ch. 3, pp. 319-325 (1 January 2010)
2. Charge Sheet
3. Enclosure 1 to Appellate Exhibit XIV (Bill of Particulars)

LEGAL AUTHORITY AND ARGUMENT

A specification is a plain, concise, and definite statement of the essential facts constituting the offense charged. RCM 307(c)(3). A specification is legally sufficient when it (1) alleges all the elements of the offense, (2) provides notice to the accused of the offense against which he must defend, and (3) gives sufficient facts to protect against re-prosecution.

See *United States v. Sell*, 11 C.M.R. 202, 206 (C.M.A. 1953). Every element must be alleged expressly or by necessary implication. RCM 307(c)(3). Specific evidence supporting the allegations ordinarily should not be included in the specifications. RCM 307(c)(3) discussion (G)(iii).

I. THE SPECIFICATION OF CHARGE I ADEQUATELY STATES AN OFFENSE.

The Specification of Charge I is legally sufficient because it alleges all the elements of the Article 104 offense in this case, either expressly or by necessary implication. The Specification contains the name, rank, and military association of the accused ("Private First Class Bradley E. Manning, U.S. Army"); the date and place of the offense ("Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 27 May 2010"); a description of the offense ("give intelligence to the enemy, through indirect means"), including the *mens rea* required ("knowingly"); and includes words indicating criminality ("without proper authority"), as required by RCM 307(c)(3). See RCM 307(c)(3) discussion (C)(i)–(ii); (D)(i), (iii); (E); (G)(i), (iii). No additional information is required to be alleged. See *id.* Further, the Government's filing of a Bill of Particulars in this case cures any notice or double jeopardy issues by identifying the enemy, the intelligence, and the indirect means. See Enclosure 3; see also RCM 906(b)(6).

The defense argues that the Specification of Charge I fails to allege a "general criminal intent." See Def. Mot. at 2-3. However, the Specification of Charge I alleges the accused "knowingly gave intelligence to the enemy" and that he did so "without proper authority." See Charge Sheet. This confusion over what is required to be alleged seems to arise from cases characterizing the nature of findings under Article 104(2). *United States v. Batchelor*, 22 C.M.R. 144 (C.M.A. 1956), is instructive on this point. In *Batchelor*, the Court of Military Appeals held that Article 104(2) does not require a specific criminal intent; thus, a law officer's instructions on the elements of Article 104(2) were correct when he characterized Article 104(2) as requiring the finding of a general criminal intent and a finding as to words importing criminality. See *Batchelor*, 22 C.M.R. at 158. Like the prosecution in *Batchelor*, the United States agrees that Article 104(2) requires a showing or finding of criminal intent—but this is wholly different than what is required to be alleged in a specification. See *id.* at 157. In this case, the United States alleged a general criminal intent by specifying that the accused acted "knowingly" and "without proper authority." See Charge Sheet. The inclusion of *mens rea* and words indicating criminality in the Specification of Charge I confirms the United States has adequately stated an offense under Article 104(2) in this case.

The defense repeatedly conflates what the United States is required to prove with what the United States is required to allege in order to adequately state an offense. This is readily apparent in the defense statement that "courts have uniformly held that the Government must allege and prove a general criminal intent to give intelligence to, or communicate with, the enemy under Article 104(2)." Def. Mot. at 3. For this proposition, the defense relies on *Batchelor*, *United States v. Anderson*, 68 M.J. 378 (C.A.A.F. 2010), and *United States v. Olson*, 22 C.M.R. 250 (C.M.A. 1957). See Def. Mot. at 3. These cases lend no support to the defense position. As discussed above, *Batchelor* held that Article 104(2) requires a finding of general criminal intent. *Anderson* and *Olson* are similarly inapplicable. The accused in *Anderson* was

charged with "Attempting to Aid the Enemy" under Article 104(1). An "attempt" under Article 104(1) requires the Government to prove a specific intent to aid the enemy as an element of the crime¹; thus, the Government could not allege any general criminal intent as contemplated by the defense. See *Anderson*, 68 M.J. at 384-85, nn. 4-7. As for *Olson*, the accused was charged with "Aiding the Enemy" under Article 104(1), not "Communicating" or "Giving Intelligence to the Enemy" under Article 104(2). *Olson*, 22 CMR at 254. Even assuming, *arguendo*, that Olson had been charged with "Communicating" under Article 104(2), "Communicating" and "Giving Intelligence" are different offenses. They have different model specifications and different elements. See *MCM*, United States, pt. IV, ¶ 28(b)(4)-(5), 28(f)(3)-(4) (2008). Model specifications are intended to guide drafters by incorporating the necessary elements, and the Specification of Charge I expressly alleges the elements for "Giving Intelligence" under Article 104(2). See *MCM*, Punitive Articles Discussion, at IV-1 (2008).

As stated above, the defense motion repeatedly emphasizes what the United States is required to prove in order to obtain a conviction. As such, this portion of the defense motion would be more appropriately styled as a motion for a finding of not guilty under RCM 917 after the close of the Government's case. See RCM 917(a). The Specification of Charge I adequately states an offense under Article 104(2).

II. ARTICLE 104, AS APPLIED, IS NOT UNCONSTITUTIONALLY VAGUE IN VIOLATION OF THE FIFTH AMENDMENT.

The defense argues that the Government's application of Article 104, including the term "indirectly," renders Article 104 unconstitutionally vague in violation of the Due Process Clause of the Fifth Amendment. See Def. Mot. at 8. In short, Article 104 is not unconstitutionally vague because an ordinary Soldier could understand what conduct was prohibited, and the application of the Article in this case does not encourage arbitrary and discriminatory enforcement.

Due process requires "fair notice" that an act is forbidden and subject to criminal sanctions. See *United States v. Bivins*, 49 M.J. 328, 330 (C.A.A.F. 1998); see also *Connally v. General Constr. Co.*, 269 U.S. 385, 391 (1926) ("A statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application violates due process."). Due process also requires fair notice as to the standard applicable to the forbidden conduct. See *Parker v. Levy*, 417 U.S. 733, 755 (1974).

In determining the sufficiency of the notice, courts must examine the law "in light of the conduct with which [an accused] is charged." *United States v. National Dairy Products Corp.*, 372 U.S. 29, 33 (1963) (citing *Robinson v. United States*, 324 U.S. 282 (1945)). There is a strong presumption of validity that attaches to an Act of Congress; hence, "statutes are not

¹ Under Article 104(a)(1), attempting to aid the enemy, the Government must prove (1) That the accused did a certain overt act; (2) That the act was done with the intent to aid the enemy with certain arms, ammunition, supplies, money, or other things; (3) That the act amounted to more than mere preparation; and (4) That the act apparently tended to bring about the offense of aiding the enemy with certain arms, ammunition, supplies, money, or other things. UCMJ art. 104(b)(2) (2008).

automatically invalidated as vague simply because difficulty is found in determining whether certain marginal offenses fall within their language.” *Jordan v. De George*, 341 U.S. 223, 231 (1951). Generally, a statute is not void for vagueness if it defines “the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement.” *Kolender v. Lawson*, 461 US 352, 357.

In *Parker*, the Supreme Court held that the standard of review for “void for vagueness” challenges to punitive Articles in the military justice system is whether “one could reasonably understand that his contemplated conduct is proscribed.” *Parker*, 417 U.S. at 754–57 (“Void for vagueness simply means that criminal responsibility should not attach where one could not reasonably understand that his contemplated conduct is proscribed.”) (citing *National Dairy Products Corp.*, 372 U.S. at 32). This standard of review provides Congress more deference in drafting laws governing the military than civilians. *See id.*, at 756 (“For the reasons which differentiate military society from civilian society, we think Congress is permitted to legislate both with greater breadth and with greater flexibility when prescribing the rules by which the former shall be governed than it is when prescribing rules for the latter.”).

A. A Soldier Could Reasonably Understand that Compromising Intelligence Through an Intermediary was Subject to Criminal Sanction in the U.S. Army.

It is “settled law that notice is determined through application of an objective test as to whether a person could ‘reasonably understand that his contemplated conduct is proscribed.’” *United States v. Saunders*, 59 M.J. 1, 10 (C.A.A.F. 2003) (citing *Parker*, 417 U.S. at 757); *see also United States v. Vaughan*, 58 M.J. 29, 41 (C.A.A.F. 2003) (Crawford, J., concurring) (“[I]t is not whether [the accused] was on notice that conduct like [his] was [punishable under Article 104], but rather, whether a reasonable enlisted person would be on notice that conduct like [the accused’s] was [punishable under Article 104].”). Courts may review the Manual for Courts-Martial, military case law, military customs and usage, and military regulations in determining whether sufficient notice was provided. *See Vaughan*, 58 M.J. at 30; *see also United States v. Boyett*, 42 M.J. 150, 153 (C.A.A.F. 1995) (noting that a court may take judicial notice of regulations as evidence of military customs).

The very language of Article 104 puts a reasonable Soldier on notice that compromising intelligence to the enemy through an intermediary would subject him or her to criminal action under the Article. Article 104 criminalizes the act of giving intelligence to the enemy, “either directly or indirectly.” *See UCMJ art. 104* (2008). The act must also be done “without proper authority.” *See id.* A reasonable Soldier would understand that sending intelligence through email to the enemy without authority, if the Soldier knew the enemy was on the other end of the transmission, constitutes “directly” giving intelligence to the enemy. A reasonable Soldier would also understand that posting intelligence on a website used by the enemy without authority, if the Soldier knew the enemy used the website, constitutes “indirectly” giving intelligence to the enemy. Although Article 104 was written long before the advent of the internet, reasonable Soldiers understand that use of the internet does not alter the common understanding of “giving.” The language of Article 104 provides sufficient notice that giving

intelligence to the enemy through the internet, without authority to do so, is a violation of the Article.

In addition to the plain reading of Article 104, Army regulations and mandatory training put every Soldier on notice that disclosing intelligence on the internet, without proper authority, may subject that individual to action under the UCMJ. Army Regulation (AR) 380-5, para. 1-21a, states that "Department of Army personnel will be subject to sanctions if they knowingly, willfully, or negligently disclose classified or sensitive information to unauthorized persons." *U.S. Dep't of Army, Reg. 380-5, Department of the Army Information Security Program* para. 1-21(a)(1) (29 September 2009). Those sanctions may include actions "taken under the UCMJ for violations of that Code and under applicable criminal law, if warranted." *Id.*, at para. 1-21(b). A Soldier could reasonably understand, certainly during a time of war, that "unauthorized persons" included enemies of the United States. This regulation provides sufficient notice to Soldiers that compromising intelligence, without proper authority, may subject an individual to criminal sanctions.

Furthermore, annual Operations Security (OPSEC) training is mandatory for all Soldiers. *See* AR 530-1, *Operations Security* para. 4-2(a)(2)(b) (19 April 2007). OPSEC training under AR 530-1 puts every Soldier on notice that compromising intelligence on the internet may subject that person to criminal sanctions. AR 530-1, para. 2-1, states that all Army personnel "will prevent disclosure of critical and sensitive information in any public domain to include but not limited to the World Wide Web." *Id.*, at para. 2-1(c). AR 530-1, para. 4-3(b), provides that "[w]hile the Internet is a powerful tool to convey information quickly and efficiently, it can also provide adversaries a potent instrument to obtain, correlate, and evaluate an unprecedented volume of aggregate information regarding U.S. capabilities, activities, limitations, and intentions." *Id.*, at para. 4-3(b). AR 530-1, Appendix E-3(a)(2)(b) states that "the Internet has become an ever-greater source of open source information for adversaries of the U.S., websites in particular...are a potentially significant vulnerability." *Id.*, at Appendix E-3(a)(2)(b). The failure to comply with AR 530-1 may subject a person to criminal sanction under the UCMJ. *See id.*, at para. 2-1(b)(2). In short, military regulations and training also provide notice to Soldiers that compromising intelligence to the enemy, without proper authority, could subject an individual to disciplinary action under the UCMJ.

Because of the plain language of Article 104, as well as the notice provided by Army regulations and mandatory training, Soldiers could reasonably understand that knowingly giving intelligence to the enemy through an intermediary was subject to criminal sanction under the UCMJ.

B. The Application of Article 104 in this Case does not Encourage Arbitrary and Discriminatory Enforcement.

The void for vagueness doctrine "focuses both on actual notice to citizens and arbitrary enforcement." *Kolender v. Lawson*, 461 U.S. 352, 357 (1983). However, courts recognize "that the more important aspect of [the] vagueness doctrine 'is not actual notice, but the other principal element of the doctrine—the requirement that a legislature establish minimal guidelines to govern law enforcement.'" *Id.*, at 357 (citing *Smith v. Goguen*, 415 U.S. 566, 574 (1974) (noting

that without minimal guidelines, a statute may permit “a standardless sweep [that] allows policemen, prosecutors, and juries to pursue their personal predilections”). A statute should aim to contain, but not wholly restrict, the exercise of some discretion in enforcement. See *Grayned v. City of Rockford*, 408 U.S. 104, 114 (1972) (“As always, enforcement requires the exercise of some degree of police judgment, but, as confined, that degree of judgment [should be] permissible.”).

Determining whether an Article may lead to arbitrary enforcement requires military courts to analyze whether an Article provides a clear standard to guide enforcement. See *United States v. Cochran*, 60 M.J. 632, 634 (N.M. Ct. Crim. App. 2004). In *Cochran*, the defense argued a Navy Instruction was void for vagueness because, *inter alia*, “[i]t [was] impossible to determine which conduct is ‘unlawful’ and therefore criminal and which is not under the order without guessing.” *Id.*, at 634. The Court denied this argument because the instruction “[d]id not encourage either arbitrary or discriminatory enforcement.” *Id.*, at 635. Requiring the “intent to induce intoxication,” the Court reasoned, “establishe[d] a clear standard against which an individual’s conduct is measured.” *Id.*, at 635.

Article 104, by its terms, does not encourage arbitrary and discriminatory enforcement. Instead, it provides clear standards by which to guide enforcement. Article 104 requires, *inter alia*, that the person “knowingly” give intelligence to the enemy. See UCMJ art. 104 (2008). This *mens rea* requirement guards against arbitrary enforcement by establishing that mere negligent disclosures or even wanton disclosures are not subject to prosecution under Article 104. In addition to the *mens rea* requirement, a Soldier must give “intelligence” to the enemy. See *id.* The requirement to give “intelligence” further narrows enforcement of the Article because intelligence “means any helpful information, given to and received by the enemy, which is true, at least in part.” See *Benchmark*, p. 323 (emphasis added). The requirement of receipt of intelligence by the enemy ensures that a prosecution will not be pursued without evidence of the enemy’s possession of the intelligence. Lastly, the Soldier must give intelligence to the enemy “without proper authority.” See UCMJ art. 104 (2008). This limitation protects the Soldier who is authorized by position or circumstance to give intelligence and ensures that only wrongful acts are pursued. The parade of hypotheticals offered by the defense, such as the argument that a discussion with a reporter regarding Post-Traumatic Stress Disorder would constitute a violation of Article 104, ignore these limiting factors and do not constitute an offense punishable under Article 104. See Def. Mot. at 9.

III. ARTICLE 104 IS NOT SUBSTANTIALLY OVERBROAD IN VIOLATION OF THE FIRST AMENDMENT.

The defense argues that the Government’s application of Article 104, including the term “indirectly,” renders Article 104 substantially overbroad in violation of the First Amendment. See Def. Mot. at 10. The defense argument has no merit.

As a practical matter, use of “indirectly” in the context of Article 104 is not novel, nor is the Government’s use of the term within the Specification of Charge 1. William Winthrop’s *Military Law and Precedents* provides the following guidance:

The modes of holding correspondence and giving intelligence already instanced have been mainly of a direct character. It was, however, the indirect modes which...principally exercised the vigilance of our military authorities. The proceeding of this sort which it was found especially necessary to denounce and prohibit was the publication in newspapers of particulars in regard to [information which] might readily be communicated to the enemy; and in several instances the offence [sic] thus committed was made the subject of charges under the [precursor to Article 104], or of trial by military commission. The publishing by way of advertisement in newspapers, of "Personals," by means of which an indirect correspondence was maintained with individuals within the enemy's lines, was also expressly prohibited.

William Winthrop, *Military Law and Precedents*, 634 (2d ed. 1920 reprint). Despite the historical basis for use of the term "indirectly" in the context of publishing intermediaries, the defense maintains that the Government's interpretation or application of Article 104 to the conduct in this case, including use of "indirectly," criminalizes a substantial amount of constitutionally protected speech. See Def. Mot. at 11. The United States disagrees.

A law may be invalidated as overbroad under the First Amendment if "a substantial number of its applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep." *United States v. Stevens*, 130 S.Ct. 1577, 1587 (quoting *Washington State Grange v. Washington State Republican Party*, 522 US 442, 449 n.6 (2008)). The Government's interpretation or application of Article 104 to the conduct in this case, including use of "indirectly," does not prohibit constitutionally protected speech. Rather, the defense mischaracterization of the Government's "interpretation" of Article 104 is misguided in that the hypotheticals they offer do not constitute an offense punishable under Article 104.

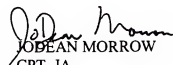
The defense argues that Article 104 "categorically prohibits any unauthorized communication with an enemy, regardless of whether the communication contains any intelligence information" and warns that the Government could prosecute an individual for "a communication that is not aimed at an enemy but may be indirectly accessed by the enemy...." Def. Mot. at 11. Aside from the fact that this example is inapplicable to the present case, as the accused was charged with "Giving Intelligence to the Enemy" not "Communicating with the Enemy," it is an inaccurate and incomplete statement of the law. The defense formulation ignores the fact that the communication must be intended to reach the enemy. See *Benchbook*, p. 324. Thus, this hypothetical raises no constitutional issues.

Likewise, the hypotheticals raised by the defense regarding information placed on the internet that "might be accessed by the enemy" are similarly inapplicable. See Def. Mot. at 11. The United States has not charged the accused under the Specification of Charge 1 with knowing that information "might be accessed by the enemy." See Charge Sheet. The United States has charged the accused with "knowingly" giving intelligence to the enemy "through indirect means." See Charge Sheet. Actual knowledge is required—not knowledge that information "might be accessed." See UCMJ art. 104(c)(5)(c) (2008). This difference invalidates all of the


defense hypotheticals involving simple discussions with reporters or the press, and extinguishes any claim that Article 104 is substantially overbroad. Further, assuming the accused under the hypothetical "knew" that by giving information to a reporter, he was giving it to the enemy – not that the accused generally knew that the enemy uses the internet or reads newspapers – the United States is still required to prove those discussions occurred "without proper authority," a fact the defense ignores. Lastly, "giving" intelligence requires that the United States prove receipt of the information by the enemy. See *Benchbook*, p. 323; Winthrop, *supra* p. 8, at 634 ("It is necessary that the enemy shall have been *actually informed*."). The defense claim that Article 104 is substantially overbroad in violation of the First Amendment is without merit.

CONCLUSION

The United States respectfully requests this Court DENY the defense motion to dismiss the Specification of Charge I for failure to state an offense. The United States also requests this Court deny the defense request to declare the term "indirectly," as used in Article 104, unconstitutionally vague in violation of the First and Fifth Amendments to the United States Constitution, or substantially overbroad in violation of the First Amendment to the United States Constitution. Finally, the United States respectfully requests this Court adopt the *Benchbook's* elements for the offense of Giving Intelligence to the Enemy under Article 104.


JODEAN MORROW
CPT, JA
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 12 April 2012.


JODEAN MORROW
CPT, JA
Trial Counsel

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

Prosecution Motion

**for Appropriate Relief to Preclude
Actual Harm or Damage from the
Pretrial Motions Practice and
the Merits Portion of Trial**

29 March 2012

RELIEF SOUGHT

The United States respectfully requests that the Court preclude the defense from raising or eliciting any discussion, reference, or argument, to include the introduction of any documentary or testimonial evidence, relating to actual harm or damage from pretrial motions related to the merits portion of trial and from the merits portion of trial. The United States does not dispute whether actual harm or damage is relevant on sentencing. The United States requests oral argument.

BURDEN OF PERSUASION AND BURDEN OF PROOF

The burden of proof on any factual issue the resolution of which is necessary to decide a motion shall be by preponderance of the evidence. See Manual for Courts-Martial, United States, Rule for Courts-Martial (R.C.M.) 905(c)(1) (2008). The burden of persuasion on any factual issue the resolution of which is necessary to decide a motion shall be on the United States as the moving party. See R.C.M. 905(c)(2). Whether the Court rules on the admissibility of evidence before it arises at trial is a decision in the discretion of the military judge. See R.C.M. 906(b)(13).

FACTS

The accused is charged with one specification of aiding the enemy, one specification of disorders and neglects to the prejudice of good order and discipline and service discrediting, eight specifications of violations of 18 U.S.C. § 793(e), five specifications of violations of 18 U.S.C. § 641, two specifications of violations of 18 U.S.C. § 1030, and five specifications of violating a lawful general regulation, in violation of Article 104, 134, and 92, Uniform Code of Military Justice (UCMJ). See Enclosure 1.

The accused is alleged to have engaged in misconduct relating to, *inter alia*, more than 127 records, files, or cables and four databases, consisting of more than 720,700 records. See id. In response, multiple government agencies and departments *immediately* began measuring what, if any, harm or damage transpired because of the alleged misconduct. Some of those agencies and departments prepared damage assessments to memorialize their findings, including the Information Review Task Force and WikiLeaks Task Force. See Enclosure 2.

On 16 February 2012, the defense submitted its Motion to Compel Discovery for the damage assessments. See Enclosure 3. The defense argued that the damage assessments were

"at odds with the classification review conducted by the OCA" and that the substance "would undercut the testimony of each Original Classification Authorities (OCAs) for the charged documents." See id. The defense concluded, both in its Motion to Compel Discovery and at the public motions hearing, that the damage assessments were material to the preparation of the defense for both the merits and sentencing, citing articles indicating that the compromised information "caused only limited damage." See id.

On 23 March 2012, the military judge ordered the United States to produce, *inter alia*, any unclassified, discoverable information from those assessments and to "immediately begin the process of producing the damage assessments that are outside the possession, custody, or control of military authorities." See Enclosure 2. The United States is in the process of producing those assessments, or portions thereof, ordered by the military judge.

Producing a damage assessment generally requires the owner of the information to engage in a four-step process: first, verify the classification of the information; second, reevaluate the classification of the information; third, determine whether there are countermeasures to minimize or eliminate the damage to national security; and fourth, prepare the actual damage assessment. See Enclosure 4.

A damage assessment measures, "given the nature of the information and the countermeasures, if any, that will be employed, [] the probable impact the compromise will [have] on our national security." Producing a damage assessment "is sometimes a long-term, multi-disciplinary analysis of the adverse effects of the compromise on systems, plans, operations, and/or intelligence." Id.

WITNESSES/EVIDENCE

The United States does not intend to produce any witnesses for this motion. The United States requests that the Court consider the following enclosures to this Motion in making its ruling.

1. Charge Sheet (enclosed in record)
2. Ruling: Defense Motion to Compel Discovery, 23 March 2012 (Appellate Exhibit XXXVI)
3. Defense Motion to Compel Discovery, 16 February 2012 (Appellate Exhibit VIII)
4. Army Regulation 380-5, Paragraph 10-5, 29 September 2000

LEGAL AUTHORITY AND ARGUMENT

The Court should preclude the defense from raising or eliciting any discussion, reference, or argument, to include the introduction of any documentary or testimonial evidence, relating to actual harm or damage from pretrial motions related to the *merits* portion of trial and from the *merits* portion of trial. Actual harm or damage is not relevant for the reasons proffered by defense, to the charges facing the accused, or to any available defenses thereto. Even if relevant, the probative value of actual harm or damage is substantially outweighed by the danger of unfair

prejudice, confusion of the issues, or misleading the members, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence. See M.R.E. 403.

I. ACTUAL HARM OR DAMAGE IS NOT RELEVANT FOR THE REASONS PROFFERED BY DEFENSE.

Evidence is relevant if it has "any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." Manual for Courts-Martial, United States, Mil. R. Evid. 401 (2008); see also M.R.E. 401, analysis ("relevant evidence must involve a fact 'which is of consequence to the determination of the action'").

The defense argued in its Motion to Compel Discovery that the damage assessments (the proffered authority which confirms whether actual harm or damage transpired) are relevant for two reasons. See Enclosure 3. First, the defense argued that the damage assessments "would undercut the testimony of each Original Classification Authorities for the charged documents." See id. The defense appears to be conflating the issues of damage and potential impact on national security. The two topics are distinct. Classification reviews are forward-thinking where the "original classification authority determines [whether] the unauthorized disclosure of the information reasonably could be expected to result in damage to national security." Exec. Order No. 13,526 § 1.2(a)(4). In contrast, damage assessments are prepared in hindsight to determine the actual impact, if any, caused by the illegal activity. See United States v. Lonetree, 31 M.J. 849, 868 (N-M C.M.R. 1990); see also Enclosure 4 (damage assessments "determine, given the nature of the information and countermeasures, if any, that will be employed, what the probable impact of the compromise will be on our national security"). Thus, the use of a damage assessment (i.e., whether damage *did* occur) to impeach an OCA who prepared a classification review (i.e., whether damage *could* occur) would be improper.

Second, the defense argued that the damage assessments were "at odds with the classification review conducted by the OCA." See Enclosure 3. Such "non-justiciable" questions, namely challenges to the classification of compromised information for which a classification review exists, are not relevant on the merits. See United States v. Huet-Vaughn, 43 M.J. 105, 114 (C.A.A.F. 1995) (the legality of the decision to employ military forces in the Persian Gulf was "irrelevant because it pertained to a non-justiciable political question"). Damage assessments may be relevant to impeach an OCA, but only if the OCA authored the document and only with respect to the assessment, not the classification review. See R.C.M. 914.

Information may be originally classified only if done so by an original classification authority. Exec. Order No. 13,526 § 1.1(a). Additionally, the information must be owned by, produced by or for, or under the control of the United States Government and must fall within one or more of the categories of following categories: military plans, weapons systems, or operations; foreign government information; intelligence activities (including covert action), intelligence sources or methods, or cryptology; foreign relations or foreign activities of the United States, including confidential sources; scientific, technological, or economic matters relating to the national security; United States Government programs for safeguarding nuclear

materials or facilities; vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or the development, production, or use of weapons of mass destruction. See Exec. Order No. 13,526 §§ 1.1(a), 1.4(a)-(h). Finally, the OCA must determine "that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security" and be able to identify or describe the expected damage. See Exec. Order No. 13,526 § 1.1(a) (emphasis added).

OCAs make their classification designations based on their authority under Executive Order 13526, Classified National Security Information (signed by President Barack Obama on 29 December 2009) or for materials classified prior to 27 June 2010 on Executive Order 12958 (signed by President Clinton on 17 April 1995 and amended by Executive Order 13292 signed by President Bush on 25 March 2003), as well as relevant classification guides.

The authority to classify information is limited to (1) the President and the Vice President; (2) agency heads and officials designated by the President; and (3) United States Government officials delegated this authority pursuant to paragraph (c) of section 1.3(a). See Exec. Order 13,526 § 1.3(a).

The President delegated the authority to make classification determinations to heads of select agencies and it remains an Executive function. Department of Navy v. Egan, 484 U.S. 518, 527 (1988) ("The authority to protect [classified] information falls on the President as head of the Executive Branch and as Commander in Chief."). The authority has been held in the relevant agencies because they have the expertise to review the information and determine the potential impact the release of that information would have on the United States as well as who can have access to that information. Id.; see, e.g., CIA v. Sims, 471 U.S. 159, 176 (1985) ("[A] court's decision whether an intelligence source will be harmed if his identity is revealed will often require complex political, historical, and psychological judgments. . . . There is no reason for a potential intelligence source, whose welfare and safety may be at stake, to have great confidence in the ability of the judges to make those judgments correctly.").

Courts largely agree that classification determinations, as products of the Executive Branch, should be presumed proper and not subject to great judicial scrutiny. See Haig v. Agee, 453 U.S. 280, 291 (1981) ("Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention"); see also Harisiades v. Shaughnessy, 342 U.S. 580 (1952) (such matters "are so exclusively entrusted to the political branches of government as to be largely immune from judicial inquiry or interference"). The decision of owner of the information must be given great deference. See Sims, 471 U.S. at 176 ("[t]he decisions of the Director, who must of course be familiar with 'the whole picture,' as judges are not, are worthy of great deference given the magnitude of the national security interests and potential risks at stake"). The Fourth Circuit provides such great deference to the classification determination that courts largely do not question the determination. See United States v. Smith, 750 F.2d 1215, 1217 (4th Cir. 1984) ("[T]he government . . . may determine what information is classified. A defendant cannot challenge this classification. A court cannot question it."), vacated and remanded on other grounds, 780 F.2d 1102 (4th Cir. 1985); see also United States v. Rosen, 487 F. Supp. 2d 703, 717 (E.D. Va. 2007) ("Of course, classification decisions are for the Executive Branch. . . .").

Even assuming, *arguendo*, the classification determination is subject to judicial scrutiny, the judicial review of this determination, much like that of a military judge's ruling, should be based on what information was before the OCA at the time of making the determination. See United States v. Phillips, 52 M.J. 268, 272 (C.A.A.F. 2000) (a judge's ruling should be reviewed based on what was available to the judge at the time of ruling). Any fact occurring after this determination, to include whether any damage actually transpired, is irrelevant.

II. ACTUAL HARM OR DAMAGE IS NOT RELEVANT TO THE CHARGES FACING THE ACCUSED.

Actual harm or damage does not "make the existence of any fact that is of *consequence to the determination of the action* more probable or less probable than it would be without the evidence." M.R.E. 401 (emphasis added). In Huet-Vaughn, the accused was charged with desertion with intent to avoid hazardous duty. See Huet-Vaughn, 43 M.J. at 114. The Government filed a motion to preliminarily exclude any evidence relating to the accused's motive for her misconduct. The trial court precluded the defense from presenting evidence relating to the accused's motive. The Court of Appeals for the Armed Forces (CAAF) agreed that such evidence was irrelevant because, *inter alia*, it did not "tend to make her [*mens rea*] more or less probable." Huet-Vaughn, 43 M.J. at 114 (the accused's motive was irrelevant to the requisite intent of the crime, thus not relevant); see also United States v. Moylan, 417 F.2d 1002, 1004 (4th Cir. 1969) (motive not relevant to element of "willful intent" in destroying board records, "but is rather an element proper for the judge's consideration in sentencing").

The law does not require the United States to prove that actual harm or damage occurred in its case-in-chief, in light of the charges facing the accused. See Enclosure 1. Actual harm or damage, including the absence thereof, is not an element, or relevant to any element, of any offense for which the accused is charged. See *id.* The extent of actual harm or damage that occurred bears absolutely no relationship to whether the accused, in fact, committed the offenses.

Charge I (Article 104, UCMJ) requires that the United States prove, *inter alia*, that the accused did "knowingly give intelligence to the enemy, through indirect means." *Id.* Actual harm or damage, including the lack thereof, caused by the misconduct is neither an element nor relevant to an element of this charge. The extent of harm or damage that transpired bears absolutely no relationship to whether the accused, in fact, committed the offense.

Specification 1 of Charge II (Article 134, UCMJ) requires that the United States prove, *inter alia*, that the accused did "wrongfully and wantonly cause to be published on the internet intelligence belonging to the United States government, having knowledge that intelligence published on the internet is accessible to the enemy, such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces." *Id.* Actual harm or damage, including the lack thereof, caused by the misconduct is neither an element nor relevant to an element of this specification. The extent of harm or damage that transpired bears absolutely no relationship to whether the accused, in fact, committed the offenses.

Specifications 2, 3, 5, 7, 9, 10, 11, and 15 of Charge II (Article 134, UCMJ) require that the United States prove, *inter alia*, that the accused had unauthorized possession of information relating to the national defense and, with reason to believe such information could be used to the injury of the United States or to the advantage of any foreign nation, did “willfully communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted, the said information, to a person not entitled to receive it, in violation of 18 U.S.C. § 793(e), such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.” *Id.* Actual harm or damage, including the lack thereof, caused by the misconduct is neither an element nor relevant to an element of these specifications. The CAAF in Diaz supports this position. See United States v. Diaz, 69 M.J. 127 (C.A.A.F. 2010).

In Diaz, the accused was charged with violating, *inter alia*, 18 U.S.C. § 793(e). The Government filed a motion *in limine* to exclude evidence which, on appeal, the defense argued could have been offered to negate the alleged “heightened *mens rea* requirement” under 18 U.S.C. § 793. The Court rejected the defense’s argument because the language of the statute, specifically that the accused “has reason to believe [that the information] *could be used to the injury of the United States*” and do so with “willfulness,” did not arise “in the context of bad intent, but in the conscious choice to communicate covered information.” *Id.*, at 132. This reasoning supported the Fourth Circuit’s decision in Morison that the government must only prove “that [the compromised information] was in fact *potentially* damaging.” United States v. Morison, 844 F.2d 1057, 1086 (4th Cir. 1988) (emphasis added). In sum, the CAAF adopted the ruling in Morison that, under 18 U.S.C. § 793(e), the United States need only prove, *inter alia*, that the accused had reason to believe the information “could be used to the injury of the United States[.]” or, put another way, that the information was “potentially damaging” – not that damage actually transpired. See Diaz, 69 M.J. at 132.

Any actual harm or damage, the existence of which may only be confirmed through witness testimony or other documentation, such as a damage assessment, is not relevant to whether select documents were classified (a fact captured through testimony relating to a classification review) and/or relate to national defense information. The extent of harm or damage that transpired bears absolutely no relationship to whether the accused, in fact, committed the offenses.

Specifications 4, 6, 8, 12, and 16 of Charge II (Article 134, UCMJ) require that the United States prove, *inter alia*, that the accused did “steal, purloin, or knowingly convert to his use or the use of another, a record or thing of value of the United States or of a department or agency thereof...of a value of more than \$1,000, in violation of 18 U.S.C. § 641, such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.” *Id.* Actual harm or damage, including the lack thereof, caused by the misconduct is neither an element nor relevant to an element of these specifications. The extent of harm or damage that transpired bears absolutely no relationship to whether the accused, in fact, committed the offenses.

Specifications 13 and 14 of Charge II (Article 134, UCMJ) require that the United States prove, *inter alia*, that the accused, “having knowingly exceeded authorized access on a Secret Internet Protocol Router Network computer, and by means of such conduct having obtained

information that has been determined by the United States government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations," did "willfully communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted the said information, to a person not entitled to receive it, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, in violation of 18 U.S.C. § 1030(a)(1), such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces." *Id.* Actual harm or damage, including the lack thereof, caused by the misconduct is neither an element nor relevant to an element of these specifications. For the reasons set forth above, any actual harm or damage, the existence of which may only be confirmed in a damage assessment, is not relevant to whether select documents were classified (a fact captured through testimony relating to a classification review) and/or relate to national defense information. The extent of harm or damage that transpired bears absolutely no relationship to whether the accused, in fact, committed the offenses.

Specifications 1-5 of Charge III (Article 92, UCMJ) require that the United States prove, *inter alia*, that the accused did "violate a lawful general regulation." *Id.* The violations include "attempting to bypass network or information system security mechanisms," "adding unauthorized software to a SIPRNET computer," "using information system in a manner other than its intended purpose," and "wrongfully storing classified information." *Id.* Actual harm or damage, including the lack thereof, caused by the misconduct is neither an element nor relevant to an element of these specifications. The extent of harm or damage that transpired bears absolutely no relationship to whether the accused, in fact, committed the offenses.

Any discussion, reference, or argument, to include the introduction of any documentary or testimonial evidence, relating to actual harm or damage is not relevant to pretrial motions related to the merits portion of trial and to the merits portion of trial. The Court should preclude any attempt by the defense to taint the proceeding with irrelevant issues during pretrial motions focused on the merits and during the merits portion that are only relevant, if at all, on sentencing. See R.C.M. 1001(b)(4); see also R.C.M. 1001(c).

III. ACTUAL HARM OR DAMAGE IS NOT RELEVANT TO ANY DEFENSE AVAILABLE TO THE ACCUSED.

Actual harm or damage does not "make the existence of any fact that is of *consequence to the determination of the action* more probable or less probable than it would be without the evidence." M.R.E. 401 (emphasis added). The extent of harm or damage that subsequently transpired bears absolutely no relationship to any legal defense, or relevant to any conceivable legal defense, available to the accused. See Huet-Vaughn, 43 M.J. at 115 (the accused's motive was "in no way a defense to this [action] and therefore [] not relevant[,] " rejecting a necessity defense and the so-called Nuremberg defense).

IV. IN THE ALTERNATIVE, THE FACTORS UNDER MRE 403 SUBSTANTIALLY OUTWEIGH ANY PROBATIVE VALUE OF ACTUAL HARM OR DAMAGE ON PRETRIAL MOTIONS RELATED TO THE MERITS PORTION OF TRIAL AND ON THE MERITS PORTION OF TRIAL.

Even assuming, *arguendo*, actual harm or damage is relevant to the merits, such evidence is substantially outweighed by those factors under MRE 403 and *Berry*. See M.R.E. 403; see also *United States v. Berry*, 61 M.J. 91, 95 (C.A.A.F. 2005) (enumerating the factors under the MRE 403 balancing test). The military judge may exclude otherwise relevant evidence, if “its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the members, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.” M.R.E. 403.

A. Permitting the Defense to Raise Unsupported Arguments Relating to Whether Actual Harm or Damage Transpired at Pretrial Motions Related to the Merits or on the Merits Will Result in Prejudice to the Integrity of the Proceeding.

MRE 403 “addresses prejudice to the integrity of the trial process, not prejudice to a particular party or witness.” *United States v. Collier*, 67 M.J. 347, 354 (C.A.A.F. 2009). The “term ‘unfair prejudice’ in the context of MRE 403 ‘speaks to the capacity of some concededly relevant evidence to lure the fact finder into declaring guilt on a ground different from proof specific to the offense charged.’” *United States v. Gaddis*, 70 M.J. 248, 254 (C.A.A.F. 2011) (citing *Old Chief v. United States*, 519 U.S. 172, 180 (1997) (analyzing the purpose behind Federal Rule of Evidence 403, which is identical to MRE 403)); see also M.R.E. 403, analysis (MRE 403 “is taken without change from the Federal Rule of Evidence”). Evidence of actual harm or damage, including lack thereof, will create “an undue tendency to suggest decision on an improper basis” and lure the fact finder into declaring guilt or innocence, irrespective of the evidence supporting the charges. See *Gaddis*, 70 M.J. at 254 (citing Fed. R. Evid. 403, advisory committee’s notes). Further, any argument by the defense that no damage occurred is inconsistent with what the United States has produced to the defense in discovery.

B. Permitting the Defense to Raise Unsupported Arguments Relating to Whether Actual Harm or Damage Transpired at Pretrial Motions Related to the Merits or on the Merits Will Result in Prejudice the United States.

If the Court permits the defense to raise or elicit unsupported arguments relating to actual harm or damage during pretrial motions practice focused on the merits and on the merits, the United States would be greatly prejudiced. See R.C.M. 906(b)(13), discussion (the purpose of a motion to make a preliminary ruling on the admissibility of evidence “is to avoid the prejudice which may result from bringing inadmissible matters to the attention of court members”). Actual harm or damage resulting from the compromised information is likely classified information. Assuming, *arguendo*, the defense continues its unsupported arguments that actual harm or damage did not occur in open court, the United States is unable to rebut the defense’s argument with classified information without satisfying the requirements for a closed session under RCM 806, assuming the government entities who own the information authorize its use. See R.C.M. 806; see also *United States v. Grunden*, 2 M.J. 116 (C.M.A. 1977). Furthermore, this would be a

new form of graymailing, whereby the government entities who own information relating to actual harm or damage would be forced to approve the use of this classified information for the sole purpose of rebutting the defense's argument, or otherwise have the prosecution be unable to answer the defense's accusations in open or closed session by protecting the information from disclosure. For these reasons, the Court should exclude actual harm or damage under MRE 403.

C. The Balancing Test under MRE 403 Confirms that the Court Should Exclude Actual Harm or Damage from Pretrial Motions Related to the Merits and to the Merits.

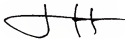
MRE 403 requires the military judge to conduct a balancing test of, *inter alia*, the strength of the proof of the fact, the probative weight of the evidence, the potential to present less prejudicial evidence, the possible distraction of the fact-finder, the time needed to prove the fact, and the presence of intervening circumstances. See *Berry*, 61 M.J. at 95. Assuming, *arguendo*, the Court finds that actual harm or damage is relevant to any pretrial motions hearing focused on the merits and on the merits, the balancing test confirms that the Court should exclude actual harm or damage from any pretrial motions hearing focused on the merits and the merits.

The Court may consider the strength of the proof of fact in conducting its balancing test under MRE 403. See *Berry*, 61 M.J. at 95. Damage assessments confirm whether, and to what extent, actual harm or damage may have occurred. However, a damage assessment is a purely hearsay statement or compilation of statements, thus likely inadmissible on its face. The strength of the proof of fact is weak, absent additional evidence to overcome hearsay. Being a classified document, the government entity that owns the information would be required to decide whether to assert the privilege under MRE 505. If the privilege is sought, a classification review would be required and the proceedings under MRE 505 would be initiated. Irrespective of whether the privilege is sought or asserted, the document is likely inadmissible on its face as pure hearsay, which may require the offering of additional evidence to overcome hearsay. Lastly, a closed hearing under RCM 806 would be required to discuss whether actual harm or damage transpired. See R.C.M. 806; see also *Grunden*, 2 M.J. at 116. Being a classified document with admissibility concerns, the time needed to prove whether actual harm or damage transpired during any pretrial motions hearing focused on the merits and during the merits may stalemate the proceeding.

The Court should also consider whether the information would operate to distract the fact finder, rather than assist in the decision-making process. See *Berry*, 61 M.J. at 95. Whether the accused's misconduct resulted in actual harm or damage would greatly distract the fact-finder from determining whether the accused committed the alleged offenses and, instead, lure the panel members to make a decision based purely on damage, not misconduct. Actual harm or damage may be a legitimate consideration of the panel on sentencing, *but not* on the merits.

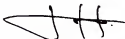
CONCLUSION

The United States respectfully requests that the Court preclude the defense from raising or eliciting any discussion, reference, or argument, to include the introduction of any documentary or testimonial evidence, relating to actual harm or damage from pretrial motions related to the merits portion of trial and from the merits portion of trial.



J. HUNTER WHYTE
CPT, JA
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 29 March 2012.



J. HUNTER WHYTE
CPT, JA
Assistant Trial Counsel

Appellate Exhibit 64
Enclosure 1
is the charge sheet

Appellate Exhibit 64
Enclosure 2
has been entered into the
record as
Appellate Exhibit 36

Appellate Exhibit 64
Enclosure 3
has been entered into the
record as
Appellate Exhibit 8

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Prosecution Motion

**for Appropriate Relief to Preclude
Actual Harm or Damage from the
Pretrial Motions Practice and
the Merits Portion of Trial**

**Enclosure #4
29 March 2012**

- (1) What is the date and identity of the article disclosing classified information?
 - (2) What specific statements in the article are considered classified and whether the data was properly classified?
 - (3) If the data came from a specific document, what is the source document's origin, and the identity of the individual responsible for the security of the classified information disclosed?
 - (4) What is the extent of dissemination of the data?
 - (5) Has the information been previously officially released?
 - (6) Was prepublication clearance sought from proper authorities?
 - (7) Have portions of, or background data on, the material, been published officially or in the open press from which an educated speculation on the consolidated data is derived?
 - (8) Can the data be declassified or otherwise made available for prosecution and, if so, what is the identity of the person competent to testify concerning its classification?
 - (9) Had declassification been decided upon before the data was published?
 - (10) What is the effect the disclosure of the classified data would have on the national security?
 - (11) Is the disclosed classified data accurate?
- f. If at any time, during the preliminary inquiry, it appears that deliberate compromise of classified information may have occurred, the situation will be immediately reported to the chain of command and supporting counterintelligence unit. Apparent violations of other criminal law will be reported to the supporting criminal investigative activity. Coordination with the command's legal counsel is recommended whenever it seems likely that administrative or other sanctions may be taken against someone because of the incident.

10-4. Reporting results of the preliminary inquiry

a. If the conclusion of the preliminary inquiry is as stated in paragraph 10-3d(2) or (4), (compromise could have occurred, or compromise did occur and damage to the national security can result) the official initiating the preliminary inquiry will immediately notify the originator of the information or material involved. If the originator was not the original classification authority, the OCA will also be immediately notified (see paragraph 10-5a, below). If the originator cannot be determined, the command's MACOM will be contacted for guidance. The MACOM will contact DAMI-CH, for those cases in which the MACOM cannot direct the command to the appropriate activity. Notification of the originator and original classification authority will not be delayed pending completion of any additional inquiry or resolution of other related issues.

b. If the conclusion of the preliminary inquiry is as stated in paragraph 10-3d(2) or (4), the command will report the matter through command channels to its MACOM, or to the Administrative Assistant to the Secretary of the Army (AASA) for offices and activities under HQDA. The MACOM or the AASA will review the report for completeness and adequacy of investigation and for the appropriateness of the corrective action/sanctions taken. Such reports will be filed and retained for a period no less than two years and are subject to HQDA or other appropriate agency oversight. MACOMs and the AASA will establish policy and procedures concerning whether or not there will be a forwarding of the reports of preliminary inquiry when the conclusion is other than stated in paragraph 10-3d(2) or (4). Reports of preliminary inquiry will be included in the Command management control review and oversight. If analysis shows that defects in the procedures and requirements of this regulation, or another Army regulation or DOD directive, contributed to the incident, MACOM, and the AASA officials will so advise DAMI-CH. DAMI-CH officials will evaluate the incident and report the conclusions, where deemed warranted, to DOD officials, if the problem concerns a DOD requirement. Report defects in the procedures and requirements regarding Army or other DOD SAPs directives, regulations, instructions, or other regulatory guidance through command channels to DAMI-CH (SAP) and DACS-DMP. If the problem concerns a DOD SAPs Directive, Instruction, or other regulatory guidance, HQDA will report to the Director, Special Programs, ODUSD(P).

c. If the conclusion of the preliminary inquiry is as stated in paragraph 10-3d(2) or (4), and foreign government information is involved, the incident will be reported through command channels and DAMI-CH to the Director of International Security Programs, ODUSD(P), who will notify the foreign government.

d. If the preliminary inquiry concludes that violations of the provisions of this regulation or criminal statutes did occur, see Chapter I, section VI, for other reporting requirements that may apply.

e. Commands will forward, through command channels to DAMI-CH, a copy or summary of the preliminary inquiry or investigation conducted, as a result of the unauthorized disclosure of classified information to the public media. An example of a preliminary report format can be found at figure 10-1, of this Chapter. DAMI-CH will forward such preliminary inquiry reports to the Director, Counterintelligence and Security Programs, OASD(C31). SAPs leak inquiries or investigations will be provided directly to DAMI-CH (SAP) and DACS-DMP, for forwarding to the Director, Special Programs, ODUSD(P) (see appendix I of this regulation and AR 380-381 for more details).

10-5. Reevaluation and damage assessment

a. When notified of possible or actual compromise, the holder of the information or material will ensure that the original classification authority, responsible for each item of the information, is notified of the incident. The OCA will verify and reevaluate the classification of the information and will conduct a damage assessment.

b. When classified information under the control of more than one command or agency is involved, the affected activities are responsible for coordinating their efforts in damage assessment and reevaluation. When participation by foreign governments or international organizations in damage assessment and reevaluation is required, contacts will be made through established intergovernmental liaison channels.

c. The first step in the reevaluation and damage assessment process is for the OCA to verify the actual, current classification of the information involved. The OCA determines whether the information currently is classified and the level and duration of classification that applies.

d. The second step is to reevaluate the classification of the information to see whether the classification should be continued or changed. This review will consider the following possibilities:

(1) The information has lost all or some of its sensitivity since it was classified, and will be downgraded or declassified. In rare cases, it might also be discovered that the information has gained in sensitivity and must be upgraded.

(2) The information has been so compromised by this incident that attempting to protect it further is unrealistic, or inadvisable, and it is to be declassified.

(3) The information must continue to be classified at the same level.

e. The third step is to determine whether there are countermeasures that can be taken to minimize or eliminate the damage to the national security that could result from the compromise. These countermeasures might include changing plans or system design features, revising operating procedures, providing increased protection to related information, through classification or upgrading, etc. The OCA performing this function is responsible for initiating or recommending the appropriate countermeasures.

f. The final step is performing the damage assessment. The OCA will determine, given the nature of the information and the countermeasures, if any, that will be employed, what the probable impact of the compromise will be on our national security. In contrast to the first three steps in this process, which must be completed quickly, this step is sometimes a long-term, multi-disciplinary analysis of the adverse effects of the compromise on systems, plans, operations, and/or intelligence.

10-6. Debriefings in cases of unauthorized access

In cases where a person has had unauthorized access to classified information, it is advisable to discuss the situation with the individual to enhance the probability that they will properly protect it. Whether such a discussion, commonly called a "debriefing," is held, is to be decided by the commander, security manager, or other designated official. This decision must be based on the circumstances of the incident, what is known about the person or persons involved, and the nature of the classified information. The following general guidelines apply:

a. If the unauthorized access was by a person with the appropriate security clearance but no need-to-know, debriefing is usually unnecessary. Debriefing is required if the individual is not aware the information is classified and that it needs protection. Inform the person that the information is classified and it requires protection. In these cases, the signing of a debriefing statement (see subparagraph e, below) is usually not necessary.

b. If the unauthorized access was by U.S. government personnel, civilian or military, without the appropriate security clearance, debriefing will be accomplished. Personnel will be advised of their responsibility to prevent further dissemination of the information and of the administrative sanctions and criminal penalties which might follow if they fail to do so. The debriefing official will make sure the individual understands what classified information is and why its protection is important.

c. If the person who had unauthorized access is an employee of a cleared contractor participating in the national industrial security program, the same guidelines apply as for U.S. Government personnel. Coordination with the employing firm's facility security officer/manager is recommended unless such coordination would place the information at increased risk.

d. If the person involved is neither U.S. government personnel, nor an employee of a cleared contractor, the decision will be made by the commander. The key question to be decided is whether the debriefing will have any likely positive effect on the person's ability and/or willingness to protect the information. As a general rule, it is often more effective in the long run to explain that a mistake occurred and that the person had unauthorized access to certain sensitive U.S. government information. Also, that such access should not have happened and that the U.S. Army needs the individual to understand that the information must be protected and never further discussed or otherwise revealed to other unauthorized personnel.

e. It is useful to have the person being debriefed sign a statement acknowledging the debriefing and their understanding of its contents. This may have a significant psychological effect in emphasizing the seriousness of the situation. If the person refuses to sign a debriefing statement, when asked, this fact, and their stated reasons for refusing, will be made a matter of record in the preliminary inquiry. The nearest counterintelligence unit will immediately be notified so that a trained CI investigator can explain the reason for the debriefing and advise the individual that a refusal to sign could indicate an unwillingness to protect classified information and could place their clearance, if held at the time, in jeopardy.

From: Fein, Ashden MAJ USA JFHO-NCR/MDW SJA
To: Lind, Denise R COL USARMY (US)
Cc: David Coombs; Kemkes, Matthew J MAJ USARMY (US); Bouchard, Paul R CPT USARMY (US); Santiago, Melissa S CW2 USARMY (US); Morrow III, JoDean, CPT USA JFHO-NCR/MDW SJA; Oversgaard, Angel M, CPT USA JFHO-NCR/MDW SJA; Whyte, Jeffrey H, CPT USA JFHO-NCR/MDW SJA; Ford, Arthur D, CW2 USA JFHO-NCR/MDW SJA; Prahler, Jay R CIV (US); Williams, Patricia CIV JFHO-NCR/MDW SJA
Bcc: Bradley, Princeton I, SGT USA JFHO-NCR/MDW SJA; Feito, Beatriz SGT USA JFHO-NCR/MDW SJA; Parra, Jairo A, WO1 USA JFHO-NCR/MDW SJA; Waybright, Daniel W, SGT USA JFHO-NCR/MDW SJA; Haberland, John CPT USA Regimental Judge Advocate
Subject: Government Motion for Appropriate Relief
Date: Thursday, March 29, 2012 8:42:00 PM
Attachments: 120329-Motion for Appropriate Relief (Enc1).pdf
120329-Motion for Appropriate Relief.pdf


Ma'am,

Attached is the government's motion for appropriate relief to preclude actual harm or damage from the pretrial motions practice and the merits portion of trial.

v/r
MAJ Fein

UNITED STATES

 y_0

MANNING, Bradley E., PFC
U.S. Army, xxx-xx-
Headquarters and Headquarters Company, U.S.
Army Garrison, Joint Base Myer-Henderson Hall,
Fort Myer, VA 22211

**DEFENSE RESPONSE
TO PROSECUTION MOTION
TO PRECLUDE REFERENCE TO
ACTUAL HARM OR DAMAGE**

DATED: 12 April 2012

1. The Defense requests that this Court deny the Government's motion in its entirety for the reasons identified herein.

2. As the moving party, the Government has the burden of persuasion. R.C.M. 905(c)(2). The burden of proof is by a preponderance of the evidence. R.C.M. 905(c)(1).

3. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of disorders and neglects to the prejudice of good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting Government property, and two specifications of knowingly exceeding authorized access to a Government computer, in violation of Articles 92, 104, and 134. UCMJ, 10 U.S.C. §§ 892, 904, 934 (2010).

4. The original charges were preferred on 5 July 2010. Those charges were dismissed by the convening authority on 18 March 2011. The current charges were preferred on 1 March 2011. On 16 December through 22 December 2011, these charges were investigated by an Article 32 Investigating Officer. The charges were subsequently referred without special instructions to a general court-martial on 3 February 2012.

LEGAL AUTHORITY AND ARGUMENT

I. The Government's Request is Premature, Internally Incoherent and Overbroad

a) The Government's Motion is Premature

5. The Government would seek to preclude the Defense from referencing at trial or in pretrial motions practice the content of damage assessments that the Defense has not yet seen and which the Government has vigorously attempted to prevent the Defense from seeing. Such a motion is premature since, if the damage assessments are not favorable for the Defense, the Defense will likely not seek to reference them during the merits or the sentencing portion of the trial. As such, the Court would be deciding a completely moot point. *See, e.g. United States v. West*, 2011 WL 856600, at * 7(N.D. Ill. Mar. 9, 2011) (court denied as premature the government's motion to preclude evidence or argument regarding a defense of duress where the motion was filed before completion of the government's document production). Although the Defense raised the concern with the Court that the Government's motion was premature, the Court has directed that the Defense respond substantively to the Government's position.¹

b) The Government's Motion is Internally Incoherent

6. It is difficult to respond to the Government's motion, as the argument is internally inconsistent. In order to respond, the Defense must make the assumption that the damage reports are favorable to the Defense, in that they show that little to no damage was caused by the alleged leaks. However, the Government continues to imply in its motion that the damage reports will show that the leaks did cause damage to national security. For instance:

- i) The Government refers repeatedly to the Defense's "unsupported arguments related to whether actual harm or damage transpired." Prosecution Motion for Appropriate Relief to Preclude Actual Harm or Damage from the Pretrial Motions Practice and the Merits Portion of Trial, p. 8 (emphasis added)[hereinafter "Government Motion"].
- ii) The Government states that "any argument by the defense that no damage occurred is inconsistent with what the United States has produced to the defense in discovery."² *Id.*
- iii) The Government states that if "the defense continues its unsupported arguments that actual harm or damage did not occur in open court" this would result in a new form of "graymail" where the Government would be forced to rebut the Defense's allegations with evidence of actual harm. Government Motion, p. 8-9.

7. Clearly, the Government's statements suggest that the damage assessments will prove that the alleged leaks caused harm or damage to the United States. If this is truly the case, why would

¹ Given that the Defense has not seen the damage assessments, it reserves the right, upon the Government providing discovery, to supplement its submissions in this Response.

² It is ironic to think that the Government is using its own discovery violations as a means to preclude the Defense from raising the issue of damage assessments.

the Defense seek to introduce evidence of damage assessments that show that the leaks did, in fact, cause damage to national security? By extension, why would the Government seek to preclude the Defense from doing something it would not do?

8. In short, the only way that the Government's motion makes any sense is to assume that the damage assessments reveal that the alleged leaks caused no harm to the United States. The Government should not be permitted to continue its practice of "smoke and mirrors" in suggesting that the damage assessments say otherwise. If they say otherwise (i.e. the alleged leaks caused harm), there would be absolutely no reason for this motion to preclude reference to them.

c) The Government's Motion is Overbroad

9. The Government requests that the Court preclude the Defense from "raising or eliciting any discussion, reference, or argument, to include the introduction of any documentary or testimonial evidence, related to actual harm or damage from pretrial motions related to the merits portion of the trial and from the merits portion of the trial." Government Motion, p. 1. It seems that the Government is not simply seeking to preclude the Defense from arguing that the alleged leaks did not cause harm, but also to preclude the Defense from referencing any "documentary or testimonial evidence[] related to actual harm or damage." (emphasis added).³ *Id.*

10. The Defense reads this to mean that the Government would seek to prevent the Defense from introducing anything that might be contained in a damage assessment from the merits portion of trial, because the damage assessment is documentary evidence "related to actual harm or damage." So if, for instance, a damage assessment provided reasons why no harm was done to the United States from the alleged leaks, the Defense would not be permitted to use that information in its case in chief. However, the reasons why the released information did not cause harm could bear on whether the information was of the type that could reasonably be expected to cause harm, as outlined in detail below.

11. The Government fails to draw a distinction between the Defense referencing the fact that the damage assessments concluded the leaks caused no harm, and the Defense referencing specific information contained in the damage assessments. The two are different things, but the Government would seek to lump them together. In either event, for the reasons discussed below, the Government's motion should be denied in its entirety because the evidence is relevant and not outweighed by the danger of unfair prejudice under M.R.E. 403.

II. The Court Should Not Preclude the Defense From Referencing a Lack of Actual Harm or the Content of the Damage Assessments

³ The Government also seeks to preclude the Defense from raising or eliciting any discussion, reference, or argument related to actual harm from pretrial motions related to the merits portion of trial. The Defense believes that this would include motions related to discovery or production as well as the current Defense Motion to Dismiss All Charges with Prejudice. Clearly, requesting the Court to order the Defense from referencing actual harm in a motion to compel discovery of the damage assessments, for instance, is ludicrous.

a) The Absence of Harm Goes to An Element of Three Offenses

12. The Government repeatedly argues that “[t]he extent of the harm or damage that occurred bears absolutely no relationship to whether the accused, in fact, committed the offenses.” See e.g. Government Motion, p. 5. Notably, the Government does not state that the absence of harm is not relevant to the charged offenses; rather, it states that “the extent of the harm or damage” is not relevant to any of the charges. This is plainly wrong on its face. If the Government chooses to show that the alleged leaks caused harm, this would be compelling proof that the leaked information could cause damage to the United States. In other words, if the Government could prove that the alleged leaks did damage to the United States, it would seem to follow that the leaks could cause damage to the United States. The Government’s failure to understand this point—and box itself into a position where it maintains harm is not relevant to the charges—is baffling.

13. It does not follow, of course, that if the alleged leaks did not cause damage, this definitively proves that they could not cause damage. However, the absence of harm is probative of whether the information leaked was of the type that the accused reasonably believed could cause harm. More specifically, the lack of harm from the leaks is relevant to the 18 U.S.C. §793 and the 18 U.S.C. §1030 offenses and whether the accused had reason to know that the information released could be used to the injury of the United States or to the advantage of a foreign nation. See Charge Sheet. Further, the lack of harm from the leaks is relevant to whether the accused acted “wantonly,” an element of the Article 134 offense. *Id.*

14. The 18 U.S.C. §793 and the 18 U.S.C. §1030 offenses require that the Government prove that “the accused had reason to believe” that the “information could be used to the injury of the United States or the advantage of any foreign nation.” *Id.* The Government seems to think that an analysis of whether the information “could” be used to the injury of the United States or the advantage of any foreign nation takes place in a vacuum. The Government conveniently overlooks that the offenses require that the Government prove the accused had “reason to believe” the information “could be used to the injury of the United States or the advantage of a foreign nation.” As such, this is not a merely hypothetical inquiry into the word “could.” Rather, the offenses require the Government to show that the accused had “reason to believe” that the information could be used to the injury of the United States. See *United States v. Truong Dinh Hung*, 629 F.2d 908, 919 (4th Cir. 1980) (approving jury instruction that “reason to believe” meant that a defendant must be shown to have known facts from which he concluded or reasonably should have concluded that the information could be used for the prohibited purposes). The Article 134 involves a similar inquiry: whether PFC Manning acted “wantonly” (i.e. highly recklessly) in causing the charged information to be published on the internet.

15. The Defense is entitled to argue that, by virtue of his expertise and training, PFC Manning knew which documents and information could be used to the injury of the United States or to the advantage of any foreign nation. PFC Manning had access to a great deal of very sensitive information that, if disclosed, could have caused damage to the United States. By selecting the information that he allegedly did, PFC Manning deliberately chose information that could not cause damage to the United States. The reasonableness of his belief that the information could not cause damage is buttressed by the damage assessments which (presumably) say that the leaks

did not cause damage to the United States. In short, the Defense submits that the damage assessments confirm that PFC Manning did not have “reason to believe” that the information could cause damage to the United States or be used to the advantage of a foreign nation. Further, the lack of damage from the leaks supports the view that PFC Manning did not act “wantonly,” an element of the Article 134 offense.

16. The Government believes that the classification level of the documents themselves is conclusive (or virtually conclusive) of whether the information could cause damage. The Government’s argument in this respect—that “[c]ourts largely agree that classification determinations, as products of the Executive Branch, should be presumed proper and not subject to great judicial scrutiny”—is misleading. See Government Motion at p. 4. The Government cites small excerpts from cases which seem to suggest that courts must defer to classification rulings, presumably in the context of deciding whether classified information could cause damage.⁴ These excerpts are misleading in that none of them deal with the issue at hand, i.e. whether classification decisions are entitled to great deference in determining whether the information could cause damage. In *United States v. Rosen*, 487 F. Supp. 2d 703, 717 (E.D. Va. 2007), the court was deciding whether it should close the trial under a novel system proposed by the government owing to the classified information involved.⁵ *United States v. Smith*, 750 F.2d 1215 (4th Cir. 1984) dealt with the admissibility of classified evidence in a proceeding. And *CIA v. Sims*, 471 U.S. 159 (1985) involved the powers of the Director of the CIA to withhold intelligence information from a Freedom of Information Act request. *Harisiades v. Shaughnessy*, 342 U.S. 580 (1981) does not even deal with classified documents or information. Instead, it deals with the constitutionality of the Alien Registration Act. The Supreme Court in that case stated:

It is pertinent to observe that any policy toward aliens is vitally and intricately interwoven with contemporaneous policies in regard to the conduct of foreign relations, the war power, and the maintenance of a republican form of government. Such matters are so exclusively entrusted to the political branches of government as to be largely immune from judicial inquiry or interference.

Id. at 588-589. Thus, the Supreme Court was not talking about classification determinations in reference to “such matters” as the Government’s citation would seem to suggest. See

⁴ Otherwise, it is not clear what the point of this discussion is.

⁵ In that case, the Court refused to adopt the government’s plan stating:

Here, the government has not met its burden; instead, it has done no more than to invoke “national security” broadly and in a conclusory fashion, as to all the classified information in the case. Of course, classification decisions are for the Executive Branch, and the information’s classified status must inform an assessment of the government’s asserted interests under *Press-Enterprise*. But ultimately, trial judges must make their own judgment about whether the government’s asserted interest in partially closing the trial is compelling or overriding. As noted, a generalized assertion of “national security interests,” whether by virtue of the information’s classified status or upon representation of counsel, is not alone sufficient to overcome the presumption in favor of open trials. Here, the government has not proffered any evidence about danger to national security from airing the evidence publicly, let alone an item-by-item description of the harm to national security that will result from disclosure at trial of each specific piece of information as to which closure is sought, as required by *Press-Enterprise*.

Id.

Government Motion at p. 4. Rather, it was talking about the United States' policy toward aliens. Similarly, the *Haig v. Agee*, 453 U.S. 280 (1981) case deals with the U.S.'s power to revoke a passport, not with whether courts should defer to classification determinations.

17. As is clear, the Government does not provide support for its proposition that classification decisions are worthy of great deference as it concerns the conclusion that classified information "could" cause harm. This is because military (and other) case law clearly establishes that the classification of a document is only probative, and not determinative, of the issue of whether information could cause harm. In *United States v. Diaz*, 69 M.J. 127 (C.A.A.F. 2010), C.A.A.F. stated:

[C]lassification alone does not satisfy the *mens rea* requirement of §793(e). Surely classification may demonstrate that an accused has reason to believe that information relates to national defense and could cause harm to the United States. However, not all information that is contained on a classified or closed computer system pertains to national defense. Likewise not all information that is marked as classified, in part or in whole, may in fact meet the criteria for classification. Conversely, information that is not so marked may meet the standards for classification and protection. This is evident enough with respect to information received through oral means or information the recipient should have reason to believe warrants protection.

Id. at 133. Under *Diaz*, the Government cannot satisfy its burden of showing that the documents could cause damage merely by pointing to their classification.⁶

18. The Government cites *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988) for the proposition that "the government must only prove 'that [the compromised information] was in fact potentially damaging.'" (Government emphasis). The Government has failed to cite the more important part of the *Morison* holding:

Though the point is to me a close one, I agree that the limiting instruction which required proof that the information leaked was either "potentially damaging to the United States or might be useful to an enemy" sufficiently remedied the facial vice. Without such a limitation on the statute's apparent reach, leaks of information which, though undoubtedly "related to defense" in some marginal way, threaten only embarrassment to the official guardians of government "defense" secrets, could lead to criminal convictions. Such a limitation is therefore necessary to define the very line at which I believe the first amendment precludes criminal prosecution, because of the interests rightly recognized in Judge Wilkinson's concurring opinion. This means, as I assume we reaffirm today, that notwithstanding information may have been classified, the government

⁶ The Government cites *Diaz* for a completely unrelated proposition that is not at issue here. See Government Motion, p. 6. The motion to preclude evidence in *Diaz* was related to intent, not relevance. In *Diaz*, the military judge excluded evidence that the Defense contended would satisfy the heightened *mens rea* requirement in 18 U.S.C. §793(e). *Id.* at 137. Given that the Court concluded there was no heightened *mens rea* requirement for 18 U.S.C. §793(e), the exclusion of the evidence was proper. This ruling does not speak at all to whether it is appropriate to exclude reference to actual harm in this case.

must still be required to prove that it was in fact “potentially damaging ... or useful,” i.e., that the fact of classification is merely probative, not conclusive, on that issue, though it must be conclusive on the question of authority to possess or receive the information. This must be so to avoid converting the Espionage Act into the simple Government Secrets Act which Congress has refused to enact.

Id. at 1086. As both *Diaz* and *Morison* demonstrate, the Government does not get a “free pass” on establishing whether information could cause damage by simply relying on the fact of classification itself. Under the 18 U.S.C. §793 and the 18 U.S.C. §1030 offenses, the Government must prove that the information could cause damage—and more specifically, that the accused had reason to know that the information could cause damage. The Defense should be entitled to rebut the allegation by showing that the accused did not have reason to believe that the information could cause damage and testing the reasonableness of that belief against the actual damage caused. Moreover, under the Article 134 offense, the Defense should be entitled to argue that PFC Manning did not “wantonly” cause intelligence information to be published on the internet. The lack of actual harm supports the view that any alleged disclosure of information was not wanton.

b) The Absence of Harm is Relevant Impeachment Evidence

19. In addition to going toward a key element of three separate offenses, the Defense maintains that the absence of damage is relevant for the impeachment of Government witnesses who claim that the leaks “could” cause damage. The Government, however, believes that the use of a damage assessment to impeach an Original Classification Authority (OCA) who prepared a classification review would be improper. Government Motion, p. 3. The Government provides no justification for its position. Why is it “improper” to use actual ex post knowledge to challenge the reasonableness or appropriateness of the ex ante classification decision which the Government relies on to show the documents could cause damage? As *Diaz* states, the classification level of the documents themselves is not determinative of whether the information “could” cause damage (or whether the accused had reason to believe they could cause damage). As such, the Defense should be able to probe the basis of a Government witness’ testimony that the information could cause damage by using ex post damage assessments. See *United States v. Israel*, 60 M.J. 485, 486 (C.A.A.F. 2005) (“A defendant’s right under the Sixth Amendment to cross-examine witnesses is violated if the military judge precludes a defendant from exploring an entire relevant area of cross-examination.”) (citing *United States v. Gray*, 40 M.J. 77, 81 (C.M.A. 1994)).

20. For instance, suppose that a damage assessment revealed that Afghani sources were not compromised in the alleged leaks; the reason is that the sources were referred to in the leaked SIGACTS by initials and not name. The Defense should be able to use this information to question the Government witness about whether, when conducting the original classification review, he or she knew that the sources were referred to by initials. This could then form the basis for impeaching the witness’ testimony that the leaks “could” cause damage. While the Government would neatly have the Court separate the OCA classification reviews from the OCA

damage assessments, the analysis is not that tidy. Evidence from the latter is directly relevant to the former and can be used to impeach a witness' credibility.

21. Moreover, the Government notes that the damage assessments look at the damage to national security given based, in part, on the nature of the information released. Government Motion at p. 2 (emphasis added). If the damage assessments conclude that the nature of the information is such that it would not cause harm, then the Defense should be able to use that information to challenge the OCAs' original determination that the information was of such a nature that it could cause harm.

IV. Reference to the Absence of Harm from the Alleged Leaks Should Not be Excluded Under M.R.E. 403

22. The Government believes that permitting the Defense to raise issues related to actual harm from the leaks (or the absence thereof) would: a) result in prejudice to the integrity of the proceeding; b) result in prejudice to the United States; c) fail the balancing test under M.R.E. 403.⁷

23. The Government makes no legitimate proffer that reference to actual harm will undermine the integrity of the trial process or cause prejudice to the Government. Indeed, the cases cited by the Government in this respect speak to prejudice to the accused—not the integrity of the process or prejudice to the United States. See, e.g., *United States v. Collier*, 67 M.J. 347, 354 (C.A.A.F. 2009) (“[T]he term ‘unfair prejudice’ in the context of M.R.E. 403 ‘speaks to the capacity of some concededly relevant evidence to lure the fact finder into declaring guilt on a ground different from proof specific to the offense charged.’”)(emphasis added) (cited in Government Motion, p. 8).

24. The Government's argument seems to be that it will suffer great prejudice for the following reason: if the Defense references the fact that the leaks did not cause damage, the Government would be forced to rebut that evidence with its own evidence that the leaks did cause damage. Since the information would be classified, this would be a new form of graymailing. The government entities who own information related to actual harm or damage would be forced to approve the use of this classified information for the sole purpose of rebutting the defense's argument.

25. The Government's argument suffers from many weaknesses. First, the Defense plans on introducing any favorable damage assessments on sentencing; thus, the Government would be in a position where—if it wanted to refute the Defense's argument—it would already have had to secure the relevant approvals. Second, the Defense is not able to reference classified information contained in the damage assessment in “open court” as the Government suggests. See Government Motion, p. 8. So all of the proceedings where the Defense or the Government referenced classified information from the damage assessments would need to be in closed proceedings in any event. Third, the Government's “graymailing” theory is ludicrous. Why

⁷ Again, the Defense would point out that it is virtually impossible to conduct a balancing test for information that the Court and the Defense has not yet seen.

would the Defense “graymail” the Government into disclosing documents or information that hurt the Defense?

26. The Government then cites miscellaneous other reasons why the Court should not allow the Defense to reference the damage assessments under M.R.E. 403: the statements are inadmissible hearsay, the documents are classified, closed sessions would be required to discuss the contents of the damage assessments. *See* Government Motion, p. 9. None of these are reasons for precluding the Defense from referencing the lack of damage caused by the leaks. The Defense would challenge the fact that these documents are inadmissible hearsay (and certainly the issue cannot be resolved as part of this motion). Further, thousands of documents in this case are classified and require approvals and closed sessions; the damage assessments are no different.

27. To the extent that there are any concerns about confusing the issues, the Court has the inherent power to control its own process. If, at the time the Defense references the damage assessment, the Court believes that the line of questioning is complicated or too attenuated, it can make the decision not to allow the Defense to continue. Moreover, if there is any confusion on this issue in the mind of the panel members, the Court can issue appropriate instructions. In short, there are simple remedies available to the Court that are far short of outright precluding the Defense from “raising or eliciting any discussion, reference, or argument, to include the introduction of any documentary or testimonial evidence, related to actual harm or damage from pretrial motions related to the merits portion of trial and from the merits portion of trial.” Government Motion, p. 1.

28. The court in *United States v. Drake*, in response to a motion by the prosecution to preclude the defense in that case from referencing certain evidence, expressed an unwillingness to foreclose a potential line of argument, especially given that the court had the inherent power to control the courtroom. The court stated in this respect:

THE COURT: -- but my point is that, to preclude them from going down that path, I think, essentially prevents them from presenting a defense, that we can control the matter of whether or not there is reference to necessity or justification, and I'm fairly confident I'll be able to control the courtroom to do that. It's just a matter of where else we go with this motion, and it seems to me they're certainly entitled to get into this.

...

THE COURT: As I interpret the Government's motion, or as I intend to interpret it, it doesn't mean that that evidence is -- although the Government seems very concerned with it amounting to a higher calling, necessity, or justification defense, I'm fairly confident that I can keep this case on track to correct you if you happen to make an inadvertent mistake in that regard, but you're certainly free to have at that in terms of the intent element, and that's how I see it.

Transcript of Record at M-100, M-103, *United States v. Drake*, No. RDB-10-181 (D. Md. Mar. 31, 2011) (emphasis added). The court's response in *Drake* was an eminently sensible one,

which recognized that there are reasonable alternatives short of outright preclusion available to address any concerns of prejudice or confusion.

CONCLUSION

29. For the reasons outlined herein, the Defense requests that this Court deny the Government's motion in its entirety. In the alternative, the Defense requests that this Court defer ruling on the motion until all relevant evidence has been produced. *See United States v. Swenson*, 51 M.J. 522, 526 (A.F. Ct. Crim. App. 1999) ("By deferring his ruling, the military judge often can better assess the relevance and necessity of the evidence.").

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. Coombs', with a stylized flourish at the end.

DAVID EDWARD COOMBS
Civilian Defense Counsel

11 April 2012

MEMORANDUM FOR RECORD

SUBJECT: Security Expert Review of Defense Motions

1. I hereby certify that I have reviewed the following Defense motions for the presence of classified information:

- a) Defense Response Motion to Prosecution's Motion to Preclude Reference to Actual Harm or Damage ; and
- b) Defense Request for Partial Reconsideration of Discovery Ruling;

I do not believe that either of these motions contains classified information or information that a reasonable person could believe to be classified.

2. The point of contact for this memorandum is the undersigned at (443) 861-9673.



CHARLES J. GANIEL
Command, SSO
HQ ATEC G-2/3/7

March 21, 2012

Via Federal Express

Colonel Denise R. Lind
Chief Judge, 1st Judicial Circuit
U.S. Army Trial Judiciary
U.S. Army Military District of Washington
Office of the Staff Judge Advocate
103 Third Avenue, SW, Suite 100
Fort McNair, DC 20319

Re: Access to Court-Martial Records in *United States v. Bradley Manning*

Dear Chief Judge Lind:

The Center for Constitutional Rights (CCR) represents the Wikileaks media organization and its publisher Mr. Julian Assange regarding access to the court-martial proceedings in *United States v. Bradley Manning* at Fort Meade, Maryland. We write to request that the Court make available to the public and the media for inspection and copying all documents and information filed in the *Manning* case, including the docket sheet, all motions and responses thereto, all rulings and orders, and verbatim transcripts or other recordings of all conferences and hearings before the Court. We have been unable to obtain access to these important documents and have been told that they are not being made available to the public, media or interested parties. As the Manning court martial purports to be a public trial, we cannot understand why critical aspects of the proceedings are being withheld from public view. As Circuit Judge Damon Keith wrote in *Detroit Free Press v. Ashcroft*, 303 F.3d 681, 683 (6th Cir. 2002): "Democracies die behind closed doors." We urge the Court to take the action required by military law and the Constitution and make these documents available.

First, there is no dispute that military law (including RCM 806) mandates a presumption of open, public court-martial trials, which may be overcome only in limited circumstances based on specific findings that closure is necessary. The public, including the media, have First Amendment and common law rights of access to criminal trials. There is also no dispute that the public has a compelling interest in obtaining access to all documents and information filed in Pfc. Manning's case given the nature of his alleged offenses. Access for media organizations, including groups such as Wikileaks which provide groundbreaking independent reporting on issues of great international significance, is especially important to ensure transparency, freedom of the press, and the integrity of these proceedings. The fairness of the proceedings have already been called into doubt by strong evidence and recent findings by United Nations Special Rapporteur on Torture, Juan Mendez, that Pfc. Manning suffered cruel, inhuman and degrading treatment – if not torture – during an 11-month period of solitary pretrial confinement in Kuwait and at Marine Corps Base Quantico.

Second, Wikileaks and Mr. Assange also have a unique and obvious interest in obtaining access to documents and information filed in this case. For more than a year, there has been intense worldwide speculation that hundreds of thousands of allegedly classified diplomatic cables published by Wikileaks – as well as *The New York Times*, *The Guardian*, and other international media organizations – were provided to Wikileaks and/or Mr. Assange by Pfc. Manning. Mr. Assange notably has a particular personal interest in this case because it appears that federal prosecutors in the Eastern District of Virginia have obtained a sealed indictment against him concerning matters that, based on prior official statements, will likely be addressed in Pfc. Manning's court-martial.

Notwithstanding these substantial interests, the *Manning* court-martial case thus far has not proceeded with the requisite openness. Instead, to date this court-martial reflects – and indeed compounds – the lack of openness experienced in Pfc. Manning's prior Article 32 hearing. Documents and information filed in the case are not available to the public anywhere, nor has the public received appropriate prior notice of issues to be litigated in the case. For example, undersigned counsel attended the motions hearing on March 15, 2012, and determined that it was not possible to understand fully or adequately the issues being litigated because the motions and response thereto were not available. Without access to these materials, the *Manning* hearings and trial cannot credibly be called open and public. We do not understand how a court-martial proceeding can be deemed to comply with the UCMJ or the Constitution unless its proceedings are accessible in a timely fashion. The public and our clients must be given access to the legal filings when filed and prior to arguments before the Court.

In addition, like the prior Article 32 hearing, it appears that a number of substantive issues are argued and decided in secret, in closed Rule 802 conferences. These important issues should be argued and decided in open court and on the record. This impedes the public's and media's right to a public trial. For example, when the undersigned was in court we were informed that the Court had signed a pre-trial publicity order apparently after a closed door 802 discussion with counsel. The argument regarding such an order, the decision and the order itself should have happened in public. This is particularly so because the order concerns what can and cannot be said to the public and press; an order of that sort should be dealt with in open court.

We therefore request that the Court order disclosure of all documents and information filed in the *Manning* case, and further implement procedures similar to those used in connection with military commission proceedings at Guantánamo Bay to ensure that information is accessible to the public in a timely and meaningful fashion. Specifically, we request that the Court enter an order requiring (a) immediate public access to all documents and information filed to date in this case, and (b) public disclosure of documents and information filed now or in the future, including disclosure of motions and responses thereto on a real-time basis, prior to argument and rulings on such motions.

We respectfully request that the Court enter such an order, or otherwise respond to this request, by Friday, March 30, 2012, in order to allow Wikileaks and Mr. Assange to seek any further judicial relief that may be necessary to protect their rights and the rights of the media and the general public.

If you have any questions, please do not hesitate to contact me.

Respectfully submitted,

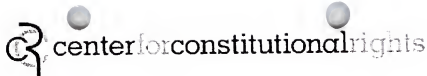


Michael Ratner
Center for Constitutional Rights
666 Broadway, 7th Floor
New York, NY 10012
Tel: (212) 614-6429
Fax: (212) 614-6499
mratner@ccrjustice.org

Counsel for Wikileaks and Julian Assange

cc: Jennifer Robinson

Jeh C. Johnson
General Counsel
Office of the General Counsel
United States Department of Defense
1600 Defense Pentagon
Room 3E788
Washington, D.C. 20301-1600



April 23, 2012

Via Email (coombs@armycourtmarshaldefense.com)

David E. Coombs, Esq.
Law Office of David E. Coombs
11 South Angell Street, #317
Providence, RI 02906

Re: *United States v. Bradley Manning*

Dear Mr. Coombs:

The Center for Constitutional Rights (CCR) represents the Wikileaks media organization and its publisher Julian Assange regarding access to the court-martial proceedings in *United States v. Bradley Manning* at Fort Meade, Maryland. We are also making this request for access on behalf of the Center for Constitutional Rights, a non-profit legal and educational organization. We ask that you forward copies of this letter to Chief Judge Lind and counsel for the prosecution in advance of the hearings commencing April 24, 2012.

By letter to Chief Judge Lind dated March 21, 2012, CCR requested public access to documents and information filed in this case, including the docket sheet, all motions and responses thereto, all rulings and orders, and verbatim transcripts or other recordings of all conferences and hearings before the Court. We have received no response to our letter, and, with the exception of certain redacted defense motions recently published on your website, continue to be denied access to the requested materials without legal justification or other explanation.

Accordingly, in order to avoid any confusion and ensure that we have exhausted efforts to obtain meaningful, timely access to documents and information filed in this case without further litigation, we now renew our request for public access to these materials, including without limitation the following items referenced in open court during the arraignment and motions hearings on February 23, March 15, 16 2012:

- All orders issued by the Court, including the case management order, pretrial publicity order, protective order regarding classified information, and other protective orders;
- The government's motion papers and responses to the redacted defense motions; and
- Authenticated transcripts of all proceedings, including in particular transcripts of open court sessions, at the same time and in the same form they are provided to counsel for the parties.

This request includes timely public access to all documents and information filed subsequent to the March 16 hearing and all such documents and information filed in the future. These should be provided when filed.

We further request that the Court require all conferences held pursuant to R.C.M. 802 be held in open court and be made part of the record in this case, to the extent they involve substantive matters, and regardless of whether the parties agree to have those substantive matters discussed and decided off the record. Moreover, we request that all Rule 802 conferences which have already occurred be reconstituted in open court.

To the extent these requests are denied (or not decided) we request an explanation for the purported factual and legal basis for such result. We expect an immediate decision as the loss of First Amendment rights in this context "for even minimal periods of time" constitutes irreparable harm. *Elrod v. Burns*, 427 U.S. 347, 373 (1976) (citing *New York Times Co. v. United States*, 403 U.S. 713 (1971)).

As you are aware, the First Amendment to the Constitution and the federal common law guarantee a right of public access to criminal proceedings, including courts-martial, except in limited circumstances. See *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, 606 (1982); *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 597 (1978). In particular, "[t]he First Amendment guarantees the press and the public a general right of access to court proceedings and court documents unless there are compelling reasons demonstrating why it cannot be observed." *Washington Post Co. v. Robinson*, 935 F.2d 282, 287 (D.C. Cir. 1991) (emphasis added) (citing cases); see also *In re Washington Post Co.*, 807 F.2d 383, 390-91 (4th Cir. 1986) (same). Access may only be denied where the government establishes that closure is necessary to further a compelling government interest and narrowly tailored to serve that interest, and the court makes specific findings on the record supporting the closure to aid review. See *Press-Enterprise Co. v. Superior Court*, 464 U.S. 501 (1984). Any motion or request to seal a document or otherwise not disclose a document to the public must be "docketed reasonably in advance of [its] disposition so as to give the public and press an opportunity to intervene and present their objections to the court." *In re Washington Post Co.*, 807 F.2d 383, 390-91 (4th Cir. 1986) (quoting *In re Knight Publishing Co.*, 743 F.2d 231, 234 (4th Cir. 1984)).

Indeed, it is reversible error for a court to withhold from the public each and every document filed, subject to further review and disclosure, because such procedures "impermissibly reverse the 'presumption of openness' that characterizes criminal proceedings 'under our system of justice.'" *Associated Press v. District Court*, 705 F.2d 1143, 1147 (9th Cir. 1983) (quoting *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 573 (1980)). It is "irrelevant" that some of the pretrial documents might only be withheld for a short time. *Id.*

The Court's authority to grant CCR's requests for public access pursuant to the All Writs Act, 28 U.S.C. § 1651(a), is equally clear and indisputable. See, e.g., *Denver Post Co. v. United States*, Army Misc. 20041215 (A.C.C.A. 2005), available at 2005 CCA LEXIS 550 (exercising jurisdiction and granting writ of mandamus to allow public access); see also *ABC, Inc. v. Powell*, 47 M.J. 363, 365 (C.A.A.F. 1997), available at 1997 CAAF LEXIS 74. This is particularly true given the Supreme Court's repeated conclusions that openness has a positive effect on the truth-determining function of proceedings and can affect outcome. See *Gannett Co. v. DePasquale*, 443 U.S. 368, 383 (1979)

("Openness in court proceedings may improve the quality of testimony, induce unknown witnesses to come forward with relevant testimony, cause all trial participants to perform their duties more conscientiously"); *Richmond Newspapers*, 448 U.S. at 596 (open trials promote "true and accurate fact-finding") (Brennan, J., concurring); *Globe Newspaper*, 457 U.S. at 606 ("[P]ublic scrutiny enhances the quality and safeguards the integrity of the factfinding process.").

Finally, senior CCR attorney Shayana Kadidal will attend the hearing in this case on April 24, 2012. We request that he be afforded the opportunity to address the Court directly and present arguments concerning our requests for public access to documents and information filed in this case.

If you, the prosecution or the Court have any questions concerning request, please do not hesitate to contact Mr. Kadidal at (212) 614-6438, shanek@ccrjustice.org, or Michael Ratner at (917) 916-4554.

Very truly yours,

Michael Ratner
Wells Dixon
Shayana Kadidal

Counsel for Wikileaks & Julian Assange

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army, xxx-xx-)

Headquarters and Headquarters Company,)

U.S. Army Garrison, Joint Base Myer-)

Henderson Hall, Fort Myer, VA 22211)

ORDER:

GOVERNMENT MOTION:

PROTECTIVE ORDER(S)

DATED: 24 April 2012

1. This Order applies when the Defense proposes to publicly release Defense Court filings or proposed filings.
2. A pleading is "filed" with the Court when it is identified as an exhibit on the record at an Article 39(a) session. Pleadings served on the opposing party that have not been identified on the record at an Article 39(a) session are "proposed filings".
3. This Order is issued IAW MRE 505(g) and (h), MRE 506(g) and (h), RCM 701(g) and RCM 806(d), and *Seattle Times v. Rhinehart*, 104 S.Ct. 2199 (1984). The Order provides procedures for the Government to request protective order(s) prior to any public release of Defense Court filings or proposed filings. The Court finds this Order necessary under the above authorities. The Government has provided the Defense both classified information and government information subject to protective order under MRE 505(g)(1) and MRE 506(g). This Court has issued a protective order for classified information provided to the Defense in discovery. The Defense accepted such discovery and agreed to comply with the protective orders. There have been two classified information spillage incidents to date in this case.
4. This Order supplements the Interim Order issued by the Court on 28 March 2012.

ORDER:

1. The Defense will notify the Government of each Defense Court filing or proposed filing intended for public release. Defense will provide the Government with the original filing and the redacted filing intended for public release.
2. Government motions for protective order will:
 - a. address each Defense Court filing or proposed Court filing individually and identify, with particularity, each portion of the filing to which the Government objects to public release and the legal basis for each objection to public release.

b. provide proposed findings of fact for the Court with respect to each portion of each filing to which the Government objects to public release.

3. Suspend Dates for Defense Court filings and proposed filings the Defense intends to publicly release. The Court is currently scheduling Article 39(a) sessions with the following schedule: 2 weeks to file motions; 2 weeks to file responses; 5 days to file replies.

a. NLT the **scheduled filing date for motions, responses, or reply** for each Article 39(a) session, the Defense shall provide the Government notice IAW paragraph (1) of this Order.

b. The Government shall provide the Court with information ordered in paragraph (2) of this Order NLT:

1. the **scheduled filing date for responses** for Defense motions;
2. the **scheduled filing date for replies** for Defense responses; and
3. **3 days** after filing of Defense replies.

The Court will grant motions for continuance for good cause.

4. The Defense will not publicly release any Defense Appellate Exhibit or proposed filing with the Court to which the Government objects until after the Government motion(s) for protective order are addressed at the next scheduled Article 39(a) session.

5. The Defense will not disclose any information known or believed to be subject to a claim of privilege under MRE 505 or MRE 506 without specific Court authorization. Prior to any disclosure of classified information, the Defense will provide notice under MRE 505(h) and follow the procedures under that rule.

6. Personal identifying information (PII) will be redacted from all Defense filings publicly released. PII includes personal addresses, telephone numbers, email addresses, first 5 digits of social security numbers, dates of birth, financial account numbers, and the names of minors.

7. To protect the safety of potential witnesses all persons who are not parties to the trial shall be referenced by initials of first and last name in any Defense filing publicly released.

So **ORDERED**: this 24th day of April 2012.



DENISE R. LIND
COL., JA
Chief Judge, 1st Judicial Circuit

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army, xxx-xx-)

Headquarters and Headquarters Company,)

U.S. Army Garrison, Joint Base Myer-)

Henderson Hall, Fort Myer, VA 22211)

**RULING: DEFENSE MOTION
TO DISMISS ALL CHARGES
WITH PREJUDICE**

DATED: 25 April 2012

Defense moves under RCM 701(g)(3)(D) to dismiss all charges with prejudice for discovery violations. The Government opposes. After considering the pleadings, evidence presented, and argument of counsel, the Court finds and concludes the following:

Factual Findings and the Law: The Court adopts the findings of fact contained in its Ruling re: Motion to Compel Discovery (AE) and the Law described therein.

Conclusions of Law:

1. In trial by general court-martial in the military justice system, charges are preferred against an accused, the charges are investigated by an Article 32 investigating officer, and forwarded with recommendations to the convening authority who makes a decision whether to refer the case to trial. RCM 307, 405, 406, 407, 504, and 601.
2. In this case the original charges were preferred on 5 July 2010 and dismissed by the convening authority on 18 March 2011. The current charges were preferred on 1 March 2011. The Article 32 investigation was held 16-22 December 2011. The convening authority referred the current charges to trial by general court-martial on 3 February 2012.
3. Unlike trials in Federal District Court, a military judge is not detailed to a court-martial until the case is referred. This case was referred on 3 February 2012. Article 26(a), UCMJ.
4. RCM 701 and RCM 703 govern discovery and production of evidence after a case has been referred for trial by the Convening Authority and a military judge has been detailed.
5. The President promulgated RCM 701 to govern discovery and RCM 703 to govern evidence production after referral. The rules work together when production of evidence not in the control of military authorities is relevant and necessary for discovery. *U.S. v. Graner*, 69 MJ 104 (C.A.A.F. 2010). The requirements for discovery and production of evidence are the same for classified and unclassified information under RCM 701 and 703 unless the Government moves for limited disclosure under MRE 505(g)(2) or claims the MRE 505 privilege for classified information. If the Government voluntarily discloses classified information to the defense, the protective order and limited disclosure provisions of MRE 505(g) apply. If, after referral, the

Government invokes the classified information privilege, the procedures of MRE 505(f) and (i) apply.

6. From the 8 March 2012 Government response to Defense Motion to Compel Discovery and its email of 22 March 2012, the Court finds that the Government believed RCM 701 did not govern disclosure of classified information for discovery where no privilege has been invoked under MRE 505. This was an incorrect belief. The Court finds that the Government properly understood its obligation to search for exculpatory *Brady* material, however, the Government disputed that it was obligated to disclose classified *Brady* information that was material to punishment only. The Court finds no evidence of prosecutorial misconduct.

7. Although the RCM and military case-law encourage early and open discovery, the Defense does not have a right to discovery under RCM 701 or *Brady* prior to referral on 3 February 2012.

8. Most of the information contained in the damage assessments requested by the Defense is maintained by other government agencies. To obtain such information from other Government agencies under RCM 703(f)(4)(A), whether discoverable under RCM 701 or not, requires the Defense to show relevance and necessity. The Government does not have authority to compel production of evidence from other government agencies under RCM 703(f)(4)(A) until after referral.

9. As the Court held in its 23 March 2012 ruling re: Motion to Compel Discovery, the fact that information controlled by another agency is discoverable under RCM 701 may make such information relevant and necessary under RCM 703 for discovery.

10. The Government has requested 13 departments, agencies, and commands to segregate and preserve records involving Wikileaks and requested information potentially discoverable from more than 50 additional agencies. This is a complex case involving voluminous classified information in the custody of multiple government agencies who have national security concerns with the disclosure of this information. As of 12 April 2012, the Government has produced 2,729 unclassified documents, consisting of 81,273 pages, and 41,550 classified documents totaling 336,641 pages. To secure this release, the Government coordinated with multiple government agencies to issue protective orders under MRE 505(g) and court orders for release of grand jury matter.

11. It is not unreasonable for Government agencies possessing potentially discoverable classified information to await the detail of a military judge to litigate issues of relevance, materiality, and necessity, and, subsequently, to litigate issues arising under MRE 505 and MRE 506 prior to releasing classified discovery to the Trial Counsel to disclose to the Defense.

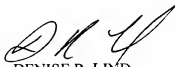
12. The Defense moved to compel the discovery it desires on 14 February 2012, 11 days after referral. On 23 March 2012, the Court ordered the Government: to immediately begin the process of producing the damage assessments for *in camera* review to assess whether they are favorable or material to the preparation of the defense under RCM 701(a)(6), RCM 701(a)(2), and *Brady*; to immediately cause an inspection of the 14 hard drives; to contact DOS, FBI, DIA, ONCIX, and CIA to determine whether any of these agencies contain any forensic results or

investigative files relevant to this case; to advise the court by 20 April 2012 whether it anticipates any government entity that is the custodian of classified information subject to the defense motion to compel will seek limited disclosure IAW MRE 505(g)(2) or claim a privilege IAW MRE 505(c); and by 18 May 2012 to disclose any favorable unclassified information from the 3 damage assessments to the Defense and all classified information from the 3 damage reports to the Court for *in camera* review.

13. The parties' proposed trial schedules anticipate trial taking place between late September and November 2012 absent the unanticipated filing of additional motions. Litigation of disputed discovery is taking place well before trial. There is no discovery or *Brady* violation in this case.

RULING: The Defense motion to Dismiss all Charges with Prejudice is **DENIED**.

So **ORDERED**: this 25th day of April 2012.



DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit

2. RCM 701(a)(2) is based on Fed. R. Crim. P. 16(a)(1)(E). Fed. R. Crim. P. 16(a)(1)(G)(3) states that Rule 16 does not apply to the discovery or inspection of a grand jury's recorded proceedings, except as provided in Fed. R. Crim. P. 6, 12(h), 16(a)(1), and 26.2.

3. Grand jury proceedings are secret. Provisions authorizing limited disclosures are governed by Fed. R. Crim. P. 6(e). The District Court where the grand jury convened may authorize disclosure preliminarily to or in connection with a judicial proceeding. A petition to disclose a grand-jury matter must be filed in the district where the grand jury convened. Fed. R. Crim. P. 6(e)(3)(E)(i) and (F).

4. As the FBI and DOJ are aligned law enforcement agencies who have participated in a joint investigation of the accused, the Government has a duty to review such investigatory files maintained by the FBI and DOJ, to include grand jury matter, for exculpatory *Brady* material and disclose the existence of such material to the Defense. If such files are under the control of another government entity, Trial Counsel must make that fact known to the Defense and engage in "good faith efforts" to obtain the material. *U.S. v. Williams*, 50 M.J. 436 (CAAF 1999).

5. RCM 914 (Production of Statements of Witnesses) provides that after a witness testifies on direct examination, the party who called the witness is required to produce any prior statements by the witness examination and use by the other party. Statements include those made by a witness to a Federal grand jury. RCM 914(f)(3).

6. Federal courts require parties seeking access to grand jury transcripts to show a particularized need and that the material they seek is necessary to avoid a possible injustice, the need for disclosure is greater than the need for continued secrecy, and the request is structured to cover only material so needed. *See U.S. v. McDavid*, 2007 WL 926664 (E.D. CA 2007); *U.S. v. Upton*, 856 F. Supp. 727 (E.D.N.Y. 1994).

Conclusions of Law.

1. Grand jury matter is not discoverable under RCM 701.

2. The Government is required to access and examine any grand jury investigation germane to the accused for exculpatory *Brady* information and disclose the existence of such information to the defense.

3. The Government is required to disclose prior grand jury statements of any government witnesses who testify IAW RCM 914. Although the rule does not require the Government to disclose such statements until after the witness has testified under direct examination, the Court will exercise its discretion under RCM 801(a)(3) to set a reasonable deadline for such disclosure in advance of trial.

4. The defense moved the Court to compel the production of the entire grand jury investigation as relevant and necessary under RCM 703(f). The defense has not demonstrated a basis for relevance and necessity, much less the particularized need required to access grand jury transcripts.

Ruling: The Defense motion to Compel production of the entire grand jury investigation involving the accused and Wikileaks is **DENIED**. The Government will examine such grand jury investigation(s) for exculpatory *Brady* material and for prior statements required to be produced under RCM 914 and will take appropriate steps under Fed. R. Crim. P. 6(e) to disclose such information to the Defense.

So Ordered this 25th day of April 2012.



DENISE R. LIND

COL, JA

Chief Judge, 1st Judicial Circuit

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

Scheduling
Order

25 April 2012

1. The Court is currently scheduling Article 39(a) sessions with the following default schedule at the request of the parties: two weeks for parties to file motions; two weeks for parties to file responses; five days for parties to file replies; and one week for the Court to review all pleadings before the start of the motions hearing. The time for filing replies was added after the first Article 39(a) session on 15-16 March 2012 because the Court received reply briefs the day before that session, the parties desire to continue to file replies, and the Court requires time to consider them.

2. Scheduling dates and suspense dates are set forth below. This schedule was coordinated with the parties. The trial schedule will be reviewed and updated as necessary at each scheduled Article 39(a) session.

a. Phase 1. Immediate Action (21 February 2012 - 16 March 2012)

b. Phase 2(a). Legal Motions excluding Evidentiary Issues (29 March 2012 - 26 April 2012)

- (A) Filing: 15 March 2012
- (B) Response: 12 April 2012
- (C) Reply: 17 April 2012
- (D) Article 39(a): 24-26 April 2012

- (1) Defense Motion to Dismiss all Charges and their Specifications with Prejudice
- (2) Government Motion for Appropriate Relief to Preclude Actual Harm or Damage from the Merits Portion of Trial
- (3) Defense Motion to Dismiss Article 104 Offense
- (4) Defense Motion to Dismiss Specification 1 of Charge II
- (5) Defense Unreasonable Multiplication of Charges Motion
- (6) Defense Renewal for Motion to Compel Discovery of Computers
- (7) Defense Renewal for Bill of Particulars
- (8) Reciprocal Discovery Requests

- (9) **MRE 404(b) Disclosures**
- (10) **Updated Proposed Case Calendar**
- (11) **Results of Hard Drive Searches to Defense in Response to Defense Motion to Compel Discovery #1**
(A) Date: 20 April 2012
- (12) **Government Notification to Court Whether Relevant Files Exist with DOS, FBI, DIA, ONCIX, and CIA**
(A) Filing: 20 April 2012
- (13) **Government Notification to Court of Whether it Anticipates Limited Disclosure or Claim of Privilege, based on (12) above**
(A) Filing: 20 April 2012
- (14) **Protective Order – Defense Publication of Its Motions**
(A) 29 March 2012/2 April 2012/12 April 2012/17 April 12 – defense notifications and redactions
(B) 17 April 2012/19 April 2012 – Government Objections and Motions for Protective Order
(C) 20 April 2012 – Defense Replies
- (15) **Defense Motion to Reconsider Compel Discovery – Grand Jury (unscheduled)**
- c. **Phase 2(b). Legal Motions (10 May 2012 - 8 June 2012)**
(A) Filing: 10 May 2012
(B) Response: 24 May 2012
(C) Reply: 29 May 2012
(D) Article 39(a): 6-8 June 2012
- (1) **Defense Motion to Dismiss All Charged Offenses under 18 U.S.C. 793(e)**
- (2) **Defense Motion to Dismiss All Charged Offenses under 18 U.S.C. 1030(a)(1)**
- (3) **Government and Defense Motions for Proposed Lesser Included Offenses**
- (4) **Defense Motion to Compel ONCIX, DOS, FBI investigation IAW RCM 701(a)(2)**
- (5) **Government Motion to Reconsider Motion to Compel DOS Damage Assessment**
- (6) **Defense Motion to Exclude Uncharged Misconduct (MRE 404(b))**
- (7) **Updated Proposed Case Calendar**

- (A) Filing: 24 May 12
- (B) Response: 29 May 12

(8) Disclosure of Unclassified Results of 3 Damage Assessment Searches to Defense in Response to the Court's Ruling, 30 March 2012

- (A): 18 May 2012

(9) Disclosure under RCM 701(g)(2) or MRE 505(g)(2) of all Information (Unclassified and Classified) to the Court in Response to the Court's Ruling, 30 March 2012

- (A): 18 May 2012

(10) Government Filing for In Camera Proceeding IAW MRE 505(i) with Notice to Defense (if Privilege is Claimed) in Response to the Court's Ruling, 30 March 2012 (Disclosure Issues)

- (A): Filing: 18 May 2012
- (B): Response: 29 May 2012
- (C): Reply: N/A
- (D): Article 39(a): 6-8 June 2012

(11) Court Rulings based on *in camera* review of damage assessments

- (A): Article 39(a): 6-8 June 2012

d. Phase 3a. Evidentiary Issues (22 June 2012 - 20 July 2012)

- (A) Filing: 22 June 2012
- (B) Response: 6 July 2012
- (C) Reply: 11 July 2012
- (D) Article 39(a): 16-20 July 2012

- (1) **Defense Motion to Compel Discovery #2 (if any)**
- (2) **Government Motion to Compel Discovery (if any)**
- (3) **Motions *in Limine* (Evidence Discovered to Date)**
- (4) **Motions to Suppress (Evidence Discovered to Date)**
- (5) **Pre-Authenticate/Pre-Admit Evidence**
- (6) **Requests for Judicial Notice**
- (7) **Witness Lists Exchanged/Compel Witnesses & Experts**
 - (A) Filing: 22 June 2012
 - (B) Government Objection to Defense Witnesses: 6 July 2012
 - (C) Motion to Compel Production: 11 July 2012
 - (D) Response: 13 July 2012

- (8) **Proposed Members Instructions for all Charged Offenses**
- (9) **Motion for Clarification of Brady material**
- (10) **Defense Notice of Intent to Disclose Classified Information under MRE 505(h)(1) (For Discovery Received – Motion to Compel #1)**
(A) Filing: 22 June 2012

- (11) **Defense Notice of Plea/Forum**
(A) Filing: 11 July 2012

- (12) **Updated Proposed Case Calendar**
(A) Filing: 6 July 2012
(B) Response: 11 July 2012

(13) **Proposed Questionnaires** – the parties will confer and arrive at a questionnaire Before the Article 39(a) session 16-20 July 2012. Issues of disagreement will be addressed at the Article 39(a) session where the questionnaire will be approved and submitted to detailed members and alternates for response NLT 3 August 2012.

e. Phase 3b. Evidentiary Issues (3 August 2012 – 31 August 2012)

- (A) Filing: 3 August 2012
(B) Response: 17 August 2012
(C) Reply: 22 August 2012
(D) Article 39(a): 27-31 August 2012
- (1) **Motions *in Limine* (Classified Information not previously Disclosed)**
- (2) **Motions to Suppress (Classified Information not previously Disclosed)**
- (3) **Article 13**
(A) Filing: 27 July 2012¹
(B) Response: 17 August 2012
(C) Reply: 22 August 2012
(D) Article 39(a): 27-31 August 2012
- (4) **Speedy Trial, including Article 10**
(A) Filing: 27 July 2012²
(B) Response: 17 August 2012

¹ The filing date of one week earlier for the defense motions is in accordance with their schedule to give the United States the necessary time to respond.

² The filing date of one week earlier for the defense motions is in accordance with their schedule to give the United States the necessary time to respond.

- (C) Reply: 22 August 2012
- (D) Article 39(a): 27-31 August 2012

(5) Pre-Qualify Experts

(6) Government Filing for In Camera Proceeding IAW MRE 505(i) with Notice to Defense (if Privilege is Claimed) in Response to the Court's Ruling, 30 March 2012 (Use as Evidence) and Other Remaining Litigation Concerning MRE 505(h) and MRE 505(i)³

(7) Production of Compelled Discovery for Defense Motion to Compel Discovery #2 or Production of Limited Discovery under MRE 505(g)(2) or (3) or Notification to Court of Claim of Privilege under MRE 505(c)

(8) Production of Compelled Discovery for Government Motion to Compel Discovery

(9) Defense Additional Witness List in light of Information in Defense Motion to Compel Discovery #2. Defense Notice of Intent to Disclose Classified Information under MRE 505(h) from Compelled Discovery #2.

(10) Updated Proposed Case Calendar

- (A) Filing: 17 August 2012
- (B) Response: 22 August 2012

f. Phase 4. Miscellaneous Motions (1 September 2012 – 21 September 2012)

(1) Any Additional Motion that does not have an Identified Deadline

- (A) Filing: 7 September 2012
- (B) Response: 14 September 2012
- (C) Article 39(a): 19-20 September 2012

(2) Grunden Hearing for all Classified Information

- (A) Filing: 7 September 2012
- (B) Response: 14 September 2012
- (C) Article 39(a): 19-20 September 2012

(3) Voir Dire Questions, Flyer, Findings/Sentence Worksheet, all CMCO

- (A) Filing for Court Review: 14 September 2012
- (B) Article 39(a): 19-20 September 2012

g. Phase 5. Trial by Members (20 September 2012 – 12 October 2012)

³ Government advised the Court will need 15 duty days to review discoverable material.

- (1) Voir Dire: 21 September 2012
- (2) Trial: 24 September 2012 – 12 October 2012

So **Ordered** this 25th day of April 2012.



DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

GOVERNMENT MOTION
FOR RECONSIDERATION
OF COURT'S RULING ON
DEPARTMENT OF STATE
DAMAGE ASSESSMENT

26 April 2012

RELIEF SOUGHT

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court reconsider a portion of its ruling, dated 23 March 2012, on the Defense Motion to Compel Discovery. The United States requests the Court make a determination that the draft Department of State damage assessment, and any information contained therein, is not discoverable because of its speculative nature.

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the United States has the burden of persuasion on any factual issue the resolution of which is necessary to decide the motion. Rule for Courts-Martial (RCM) 905(c)(2). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

FACTS

In its ruling dated 23 March 2012, the Court ordered the Government to disclose all unclassified and classified information from the Department of State damage assessment to the Court for *in camera* review under RCM 701(g)(2), or claim a privilege with respect to the classified information in the draft damage assessment. The Court also ordered the Government to identify what unclassified and classified information from the draft Department of State damage assessment was favorable to the accused and material to guilt or punishment. In its ruling, the Court found that the draft Department of State damage assessment was relevant and necessary for the Court to conduct an *in camera* review to determine whether it contains information that is favorable to the accused and material to guilt or punishment under Brady v. Maryland, 373 U.S. 83 (1963), or information relevant and favorable to the accused under RCM 701(a)(6).

On 25 April 2012, the Department of State provided a cover letter with the draft assessment for the Court's determination. See Enclosure 1. This letter provides background on the damage assessment, and the prosecution has the authority to disclose the letter to the defense counsel, but not the accused. The Department of State has not authorized the prosecution to disclose Enclosure 2 to the defense or accused, therefore it is submitted to the Court *ex parte*.

WITNESSES/EVIDENCE

1. Cover Letter, dated 25 April 2012 (classified "CONFIDENTIAL//NOFORN").
2. Enclosure to Cover Letter (classified "SECRET//NOFORN") and submitted *ex parte*.

LEGAL AUTHORITY AND ARGUMENT

Under RCM 701(g)(2), a military judge may order that discovery be denied. Upon motion of a party, the military judge may permit the party to make such a showing related to discovery, in whole or in part, in writing to be inspected only by the military judge. In this case, the Court has already ruled that the draft Department of State damage assessment be produced for its *in camera* review. The prosecution does not presently have the authority to produce the draft or any portion thereof to the defense or the accused.

A document that is preliminary, challenged, or speculative is not subject to discovery, even if it contains information that is potentially favorable to the accused and material to guilt or punishment. See Giles v. Maryland, 386 U.S. 66, 98 (1967) (Fortas, J., concurring). The draft damage assessment produced by the Department of State is a preliminary assessment of the damage caused by the WikiLeaks disclosure of Department of State diplomatic cables. See Enclosures 1 and 2. As a draft, the document is preliminary and speculative in nature, which should be apparent when reviewing the actual draft. The document does not represent the current assessment of the Department of State, merely a snapshot during a specific period of time. Although a draft document could contain information which is derived from final products, the draft itself cannot be information favorable to the accused and material to guilt or punishment because it does not in any way represent the current or past final assessment of the Department as a whole, or specific individuals in part.

If the Court finds the draft damage assessment, or any information contained within, is subject to a Brady review, pursuant to the Court's order, dated 23 March 2012, then the prosecution will review the document to identify RCM 701(a)(6) and Brady material and coordinate with the Department of State to meet the Court's 18 May 2012 suspense.

CONCLUSION

The United States requests the Court reconsider, in part, its Order dated 23 March 2012 with respect to the draft Department of State damage assessment and determine the draft assessment is not discoverable.



ASHDEN FEIN
MAJ, JA
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs,
Civilian Defense Counsel, without Enclosure 1, on 26 April 2012.



ASHDEN FEIN
MAJ, JA
Trial Counsel

Appellate Exhibit 71

Enclosure 1

2 pages

classified

"CONFIDENTIAL"

ordered sealed for Reason 3

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Appellate Exhibit 71

Enclosure 2

48 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

**Prosecution Brief
Discussing Investigations and
Damage Assessments**

26 April 2012

The United States respectfully submits this brief for the Court's consideration.

SUMMARY

Investigations can be broken down into two general categories: criminal and administrative. Criminal investigations are concerned with discovering evidence and finding the individual responsible for the crime. Administrative investigations encompass fact finding inquiries. Both criminal and administrative investigations comprise searches for information to aid making factual determinations. Damage assessments, however, as multi-discipline, multi-agency, lengthy inquiries, consider the effects of compromised classified information to reach strategic opinions.

DISCUSSION

Criminal investigations seek to discover the perpetrator of the crime and assign liability. An inquiry becomes a criminal investigation when it is conducted with a view toward discovering evidence to be used in the prosecution of a criminal action. *See United States v. Goldfinch*, 41 C.M.R. 500, 507 (A.C.M.R. 1969) (determining that inclusion of CID participation at inception of a health and safety inspection turned the search into a criminal investigation concerned with prosecution). *Williams* also contemplates investigations being oriented towards discovery of the responsible individual. *See United States v. Williams*, 50 M.J. 436, 443 (C.A.A.F. 1999) (stating that the *Brady* line of cases requires the prosecution to review records directly related to the subject of the prosecution absent a specific defense request identifying the entity, type of records, and type of information). Furthermore, *Williams* discusses criminal investigations in terms of proceedings designed to assign criminal liability. *See United States v. Williams*, 47 M.J. 621, 626 (A. Ct. Crim. App. 1997), *aff'd*, 50 M.J. 436 (C.A.A.F. 1999) ("A trial counsel's duty to disclose . . . includes information which the trial counsel has personal knowledge of or is known to criminal investigators or others that are working on the case being investigated and prosecuted.") (emphasis added). Ultimately, the fact finder reaches a factual determination based on the evidence gathered in the criminal investigation. *United States v. Augspurger*, 61 M.J. 189, 191 (C.A.A.F. 2005).

Administrative investigations are designed to find facts. *See, e.g., U.S. Dep't of Army Reg. 15-6, Procedures for Investigating Officers and Boards of Officers*, para. 1-5(a) (2 Oct. 2006) ("An administrative fact-finding procedure under this regulation may be designated an

investigation or a board of officers.”) (AR 15-6). Nevertheless, administrative actions are considered separate from criminal investigations¹ because they serve distinct purposes. *United States v. Turner*, 33 M.J. 40, 41 (stating that administrative inspections determine the fitness and readiness of a unit and are therefore unlike searches for evidence as part of the criminal justice process). Similarly, the results stemming from the investigation also distinguish criminal and administrative investigations. *United States v. Bickel*, 30 M.J. 277, 285 (C.M.A. 1990) (differentiating between actions that result in admonitions or adverse administrative actions and those resulting in criminal prosecution). Despite these differences, similar to a judicial proceeding’s verdict, administrative investigations make recommendations based upon the facts of the investigation. See AR 15-6 para. 3-11 (“Each recommendation, even a negative one . . . must be consistent with the findings.”).

Army and Department of Defense (DOD) regulations also discuss investigations in terms of locating relevant facts and persons responsible for compromised or lost classified information. See *U.S. Dep’t of Army Reg. 380-5, Department of the Army Information Security Program*, para. 10-1(a) (29 Sept. 2000) (AR 380-5); *Dep’t of Defense Regulation 5200.1-r, Information Security Program*, 10-100(a) (Jan. 1997) (DOD 5200.1-r); see also *U.S. Dep’t of Army Reg. 381-20, The Army Counterintelligence Program*, para. 4-2 (15 Nov. 1993). AR 380-5 and DOD 5200.1-r investigations are both search oriented—they operate to determine who contributed to losing or compromising classified information and fact finding related thereto. See AR 380-5 para. 10-1(a)(1)–(2) (requiring the investigation to determine whether the classified information was compromised and what persons, situations, and/or conditions contributed to the incident); DOD 5200.1-r 10-100(b)–(c). To meet the regulatory goals of limited scope, investigations under AR 380-5 and DOD 5200.1-r must be conducted promptly to ensure results are reported promptly. See AR 380-5 para. 10-1(a); DOD 5200.1-r 10-100(a). Moreover, investigations under AR 380-5 do not foreclose separate actions relating to the same incident. See AR 380-5 para. 10-1(b).

Damage assessments can relate to the same incident as an investigation; however, damage assessments are distinct from investigations because they are strategic, long-term analyses and not fact finding or criminal endeavors. See, e.g., AR 380-5 para. 10-5(f); but see *United States v. Lonetree*, 35 M.J. 396, 403 (C.M.A. 1992).² Damage assessments remain separate and distinct from classification reviews, which are performed in support of a prosecution, and from damage control, which is performed immediately after the discovery or disclosure of the compromise of classified information. See *Dep’t of Defense Instruction 5240.11, Damage Assessments*, Encl. 2 para. E2.1.4 (23 Dec. 1991) (DOD 5240.11).

¹ Although, administrative investigations are distinct from criminal investigations because they are fact finding rather than judicial proceedings, administrative investigations can transition into criminal ones based on the results of the investigation. *United States v. Cohen*, 63 M.J. 45, 51-52 (C.A.A.F. 2006) (noting that instruction contemplated the possibility that the investigation could transition into a criminal one from an administrative one).

² In dicta, *Lonetree* refers to a damage assessment as a “damage-assessment investigation.” *Lonetree*, 35 M.J. at 403. However, the *Lonetree* held the damage assessment was not a criminal investigation for purposes of determining whether the accused was entitled to an Article 31(b) warning because it was not coordinated with the military criminal investigation. *Id.* at 404. Also, the court uses the term “damage assessment” to refer to a series of interviews with a single person, the accused, and this usage is inconsistent with the manner in which the term is used in the case against the accused and in the cited laws and regulations.

Additionally, regulations treat damage assessments separately from investigations because the two are considered separately in different sections of Army and DOD regulations. Compare AR 380-5 para. 10-1 with AR 380-5 para. 10-5; and compare DOD 5200.1-r 10-100 with DOD 5200.1-r 10-104 (directing the reader to complete a damage assessment in accordance with DOD 5240.11).

Specifically, damage assessments are “a long-term, multi-disciplinary analysis of adverse effects of the compromise on systems, plans, operations, and/or intelligence.” AR 380-5 para. 10-5(f). Accordingly, the Counterintelligence Enhancement Act of 2002 (CI Enhancement Act) labels damage assessments “strategic analyses” and not “investigations.” Counterintelligence Enhancement Act of 2002, 50 U.S.C. § 402c(d)(4). The CI Enhancement Act additionally authorizes the Office of the National Counterintelligence Executive (NCIX) to conduct damage assessments but prohibits it from carrying out investigations. See *id.* at § 402c(d)(4), (6) (prohibiting NCIX from conducting counterintelligence investigations or operations). Unlike the rapid response of damage control, damage assessments are typically conducted post-prosecution. *Id.* (stating that damage assessments should be conducted after a prosecution unless special circumstances necessitate a pre-prosecution assessment). Conducting damage assessments post-prosecution comports with the time requirements required to determine in great detail the practical effects of a compromise on operations, systems, materials, and intelligence. See *id.* Upon completion, the analyses of intelligence systems in a damage assessment are delivered to security decision-makers. See *Office of the National Counterintelligence Executive, The National Counterintelligence Strategy of the United States* at 10 (Mar. 2005). Ultimately, the opinions presented in the damage assessments shape future intelligence policy at a national level. See *id.*

CONCLUSION

Based on the above, the United States submits that the term “investigation” does not include damage assessments. Whereas investigations pursue facts and conclusions based thereon, damage assessments look at the strategic effects of lost or stolen classified information. Damage assessments are conducted without an eye toward prosecution, unlike criminal prosecutions, or without a strict fact finding purpose, unlike administrative investigations. Employing multiple disciplines and multiple agencies, damage assessments expansively analyze more than facts—they analyze systems, operations and plans. Significantly, the theories damage assessments dictate policy. Contrastingly, investigations simply determine details to reach factual conclusions.

Alexander von Elten

ALEXANDER VON ELTEN
ILT, JA
Assistant Trial Counsel

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC
HHC, U.S. Army Garrison
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

CLASSIFIED INFORMATION
SEAL ORDER

26 April 2012

1. A portion of AE LXXI (71) (Enclosure 1) contains classified information as defined in MRE 505(b). The enclosure is classified at the CONFIDENTIAL/NOFORN level. This portion of the exhibit will be sealed in the record of trial in accordance with RCM 1103A, RCM 1104(b)(1)(D), and MRE 505.
2. The Court Security Officer shall cause a proper security classification to be assigned to the record of trial, to each classified exhibit, and to each page of the record of trial in which classified information appears, in accordance with RCM 1103(h). The Court Security Officer will ensure that the sealed exhibits are properly marked, including an annotation on each, that the material was sealed by order of the military judge prior to insertion into the original record of trial. Trial counsel will clearly identify in the record of trial where classified exhibits and pages in the record of trial will be maintained.
3. This portion of the exhibit contains classified national security information. This classified information shall be handled in a manner consistent with Executive Order 13526. An individual's access to the classified information in this exhibit is subject to the following: having the appropriate security clearance; signing an approved nondisclosure agreement; having a need-to-know the information; and acknowledging the Judicial Protective Order for Classified Information, dated 16 March 2012.
4. Sealed exhibits will not be opened or examined except for the following:
 - a. Prior to authentication of the record by the military judge, sealed materials may be examined upon order from the military judge based on good cause.
 - b. After authentication and prior to disposition of the record of trial pursuant to RCM 1111, sealed materials may be examined upon order issued from the military judge upon a showing of good cause at a post-trial Article 39(a) session directed by the Convening Authority.
 - c. Reviewing and appellate authorities meeting the criteria in paragraph 3 may examine sealed matters when those authorities determine that such action is reasonably necessary to a proper fulfillment of their responsibilities under the Uniform Code of Military Justice, the Manual for Courts-Martial, governing directives, instructions, regulations, and applicable rules of professional responsibility.
5. No person authorized to examine sealed exhibits shall photocopy, photograph, duplicate, or disclose the contents of the sealed exhibit in the absence from an order by a military judge, the Judge Advocate General or designee, or an appellate court, or other court of competent jurisdiction.

ORDERED, this the 26th day of April 2012.



DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC
HHC, U.S. Army Garrison
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

CLASSIFIED INFORMATION
SEAL ORDER

26 April 2012

1. A portion of AE LXXI (71) (Enclosure 2) contains classified information as defined in MRE 505(b). The enclosure is classified at the SECRET//NOFORN level. This portion of the exhibit will be sealed in the record of trial in accordance with RCM 1103A, RCM 1104(b)(1)(D), and MRE 505.
2. The Court Security Officer shall cause a proper security classification to be assigned to the record of trial, to each classified exhibit, and to each page of the record of trial in which classified information appears, in accordance with RCM 1103(h). The Court Security Officer will ensure that the sealed exhibits are properly marked, including an annotation on each, that the material was sealed by order of the military judge prior to insertion into the original record of trial. Trial counsel will clearly identify in the record of trial where classified exhibits and pages in the record of trial will be maintained.
3. This portion of the exhibit contains classified national security information. This classified information shall be handled in a manner consistent with Executive Order 13526. An individual's access to the classified information in this exhibit is subject to the following: having the appropriate security clearance; signing an approved nondisclosure agreement; having a need-to-know the information; and acknowledging the Judicial Protective Order for Classified Information, dated 16 March 2012.
4. Sealed exhibits will not be opened or examined except for the following:
 - a. Prior to authentication of the record by the military judge, sealed materials may be examined upon order from the military judge based on good cause.
 - b. After authentication and prior to disposition of the record of trial pursuant to RCM 1111, sealed materials may be examined upon order issued from the military judge upon a showing of good cause at a post-trial Article 39(a) session directed by the Convening Authority.
 - c. Reviewing and appellate authorities meeting the criteria in paragraph 3 may examine sealed matters when those authorities determine that such action is reasonably necessary to a proper fulfillment of their responsibilities under the Uniform Code of Military Justice, the Manual for Courts-Martial, governing directives, instructions, regulations, and applicable rules of professional responsibility.
5. No person authorized to examine sealed exhibits shall photocopy, photograph, duplicate, or disclose the contents of the sealed exhibit in the absence from an order by a military judge, the Judge Advocate General or designee, or an appellate court, or other court of competent jurisdiction.

ORDERED, this the 26th day of April 2012.



DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit



DEPARTMENT OF THE ARMY
U.S. ARMY TRIAL DEFENSE SERVICE
FORT LEAVENWORTH FIELD OFFICE
FORT LEAVENWORTH, KANSAS 66027-2313

ATZL-SJA-TD

23 April 2012

1. U.S. v. Giles, 386 U.S. 66 (1967)
 - a. Police reports. One included interviews with the complaining witness, as well as another key government witness. Said interviews included statements that were inconsistent with trial testimony.
 - b. Case was remanded. Court did not hold that "preliminary, challenged or speculative" information need not be disclosed.
 - c. No military justice cases cite the language quoted by the government.
2. Levin v. Clark, 408 F.2d 1209 (C.A. D.C. Cir. 1967)
 - a. Giles mentioned only in a separate statement on rehearing en banc.
 - b. "Where government's grand larceny case was based on testimony that defendant had received \$35,000 from union in small bills obtained at bank after defendant had refused \$1,000 bills, government's failure to reveal to defense a bank officer's statement which might have enabled defense to procure statements from bank personnel that no exchange of bills had taken place entitled defendant to new trial."
3. Crowder v. U.S., 294 F.Supp. 291 (E.D.MI 1967)
 - a. Cites Giles
 - b. Witness indicated before trial that he would recant his story
4. Davis v. Heyd, 350 F.Supp. 958 (E.D.LA 1972)
 - a. Cites Giles
 - b. Witness statements
5. Layman v. Tollett, 357 F.Supp. 914 (E.D.TN 1972)
 - a. Cites Giles, but notes that the Court did not agree on an opinion
 - b. Prosecution notes and memoranda
6. U.S. v. Brewer, 367 F.Supp. 156 (S.D.N.Y. 1973)
 - a. Cites Giles
 - b. Witness statements
7. U.S. v. Agurs, 427 U.S. 97 (1976)
 - a. Background information on victim, which would have tended to support the theory that the accused acted in self-defense.
 - b. Accused not deprived of fair trial because she did not request the information and it gave no inference of perjury.
 - c. The Court did note: "Because we are dealing with an inevitably imprecise standard, and because the significance of an item of evidence can seldom be predicted accurately until the

entire record is complete, the prudent prosecutor will resolve doubtful questions in favor of disclosure," at 108.

d. Giles appears only in a footnote.

8. U.S. v. Dansker, 449 F.Supp. 1057 (D.N.J. 1977)

a. Evidence related to witness credibility

9. U.S. v. Peltier, 553 F.Supp. 890 (D.N.D. 1983)

a. Documents reporting preliminary autopsy findings, the possible involvement and presence of other people, and various descriptions of the vehicle the agents followed

10. Stano v. Dugger, 883 F.2d 900 (C.A. 11th Cir., 1989)

a. One officer's belief that the accused falsely confessed. Said officer's opinion differed from the other detectives, his superiors and the state attorney.

11. U.S. v. Diaz, 922 F.2d 998 (C.A. 2d Cir., 1990)

a. Government suspected witness of theft, but did not have actual knowledge of the theft until after the trial.

12. U.S. v. Amiel, 95 F.3d 135 (C.A. 2d Cir., 1996)

a. A discredited Government witness identified another witness as an affiliate of organized crime. The prosecution interviewed the second witness and found nothing to support the allegation. The Government did not turn over the interview.

13. Shaut v. Bennet, 289 F.Supp.2d 354 (W.D.N.Y. 2003)

a. Cites Diaz

b. Pre-sentence report, including witnesses statements

14. U.S. v. Jackson, 2006 WL 3022974 (N.D.Ohio)

a. Cites Diaz

b. Audio recording between two witnesses, which was inaudible.

15. Diaz v. Smith, 2007 WL 946196 (S.D.N.Y.)

a. Cites Augurs

b. Unconfirmed allegations against officer involved in Petitioner's case were made on date of sentencing. Allegations were investigated, officer was arrested and Defense was informed.

16. U.S. v. Eubanks, Bowan & Simpson, 1997 WL 401667 (S.D.N.Y.)

a. Cites Amiel

b. Three pre-trial investigations

17. U.S. v. Gotti, 171 F.R.D. 19 (E.D.N.Y. 1997)

a. Cites Amiel

b. Witness affidavits

18. Cabrera v. Artus, 2008 WL 4146362 (E.D.N.Y.)

a. Cites Amiel

b. Government did not disclose information related to another crime, also featuring guns and bicycles, that occurred after the crime for which Petitioner was convicted.

19. DeChirico v. Walker, 558 F.Supp.2d 355 (E.D.N.Y. 2008)

a. Cites Amiel

b. False report by witness that was not known until after the witness testified.

c. Case indicates that it is "arguable" whether such information is discoverable under Amiel, though a better practice would have been to disclose. See Augur

20. U.S. v. Neeley, 308 Fed.Appx. 870 (C.A. 6th Cir., 2009)

a. Cites Amiel

b. Investigation was not disclosed

21. U.S. v. Sessa, 2011 WL 256330 (E.D.N.Y.)

a. Cites Amiel

b. Police investigation reports containing witness statements that could be used for impeachment

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC
HHC, U.S. Army Garrison
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

CLASSIFIED INFORMATION
SEAL ORDER

DATED: 26 Apr 2012

1. A portion of AE LVII (57) (Attachment E) contains classified information as defined in MRE 505(b). The attachment is classified at the SECRET//REL ACGU level. This portion of the exhibit will be sealed in the record of trial in accordance with RCM 1103A, RCM 1104(b)(1)(D), and MRE 505.

2. The Court Security Officer shall cause a proper security classification to be assigned to the record of trial, to each classified exhibit, and to each page of the record of trial in which classified information appears, in accordance with RCM 1103(h). The Court Security Officer will ensure that the sealed exhibits are properly marked, including an annotation on each, that the material was sealed by order of the military judge prior to insertion into the original record of trial. Trial counsel will clearly identify in the record of trial where classified exhibits and pages in the record of trial will be maintained.

3. This portion of the exhibit contains classified national security information. This classified information shall be handled in a manner consistent with Executive Order 13526. An individual's access to the classified information in this exhibit is subject to the following: having the appropriate security clearance; signing an approved nondisclosure agreement; having a need-to-know the information; and acknowledging the Judicial Protective Order for Classified Information, dated 16 March 2012.

4. Sealed exhibits will not be opened or examined except for the following:

a. Prior to authentication of the record by the military judge, sealed materials may be examined upon order from the military judge based on good cause.

b. After authentication and prior to disposition of the record of trial pursuant to RCM 1111, sealed materials may be examined upon order issued from the military judge upon a showing of good cause at a post-trial Article 39(a) session directed by the Convening Authority.

c. Reviewing and appellate authorities meeting the criteria in paragraph 3 may examine sealed matters when those authorities determine that such action is reasonably necessary to a proper fulfillment of their responsibilities under the Uniform Code of Military Justice, the Manual for Courts-Martial, governing directives, instructions, regulations, and applicable rules of professional responsibility.

5. No person authorized to examine sealed exhibits shall photocopy, photograph, duplicate, or disclose the contents of the sealed exhibit in the absence from an order by a military judge, the Judge Advocate General or designee, or an appellate court, or other court of competent jurisdiction.

ORDERED, this the 25th day of April 2012.



DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.


MANNING, Bradley E., PFC
HHC, U.S. Army Garrison
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

CLASSIFIED INFORMATION
SEAL ORDER

DATED: 26 Apr 2012

1. A portion of AE LVII (57) (Attachments C and D) contains classified information as defined in MRE 505(b). The attachments are classified at the SECRET//NOFORN level. This portion of the exhibit will be sealed in the record of trial in accordance with RCM 1103A, RCM 1104(b)(1)(D), and MRE 505.
2. The Court Security Officer shall cause a proper security classification to be assigned to the record of trial, to each classified exhibit, and to each page of the record of trial in which classified information appears, in accordance with RCM 1103(h). The Court Security Officer will ensure that the sealed exhibits are properly marked, including an annotation on each, that the material was sealed by order of the military judge prior to insertion into the original record of trial. Trial counsel will clearly identify in the record of trial where classified exhibits and pages in the record of trial will be maintained.
3. This portion of the exhibit contains classified national security information. This classified information shall be handled in a manner consistent with Executive Order 13526. An individual's access to the classified information in this exhibit is subject to the following: having the appropriate security clearance; signing an approved nondisclosure agreement; having a need-to-know the information; and acknowledging the Judicial Protective Order for Classified Information, dated 16 March 2012.
4. Sealed exhibits will not be opened or examined except for the following:
 - a. Prior to authentication of the record by the military judge, sealed materials may be examined upon order from the military judge based on good cause.
 - b. After authentication and prior to disposition of the record of trial pursuant to RCM 1111, sealed materials may be examined upon order issued from the military judge upon a showing of good cause at a post-trial Article 39(a) session directed by the Convening Authority.
 - c. Reviewing and appellate authorities meeting the criteria in paragraph 3 may examine sealed matters when those authorities determine that such action is reasonably necessary to a proper fulfillment of their responsibilities under the Uniform Code of Military Justice, the Manual for Courts-Martial, governing directives, instructions, regulations, and applicable rules of professional responsibility.
5. No person authorized to examine sealed exhibits shall photocopy, photograph, duplicate, or disclose the contents of the sealed exhibit in the absence from an order by a military judge, the Judge Advocate General or designee, or an appellate court, or other court of competent jurisdiction.

ORDERED, this the 25th day of April 2012.


DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)	
)	RULING: DEFENSE MOTION
v.)	TO DISMISS – UNREASONABLE
)	MULTIPLICATION OF CHARGES
MANNING, Bradley E., PFC)	
U.S. Army, xxx-xx- [REDACTED])	
HHC, U.S. Army Garrison)	
Joint Base Myer-Henderson Hall)	DATED: 25 April 2012
Fort Myer, Virginia 22211)	

Defense moves to dismiss certain charges and specifications based upon unreasonable multiplication of charges (UMC). Government opposes. After considering the pleadings, the classified enclosure presented by the defense, and argument of counsel, the Court finds and concludes the following:

Findings of Fact: The Government stipulates to the facts set forth in the Defense motion, with a singular exception. The Court adopts the following relevant facts:

1. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of conduct prejudicial to good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting government property, and two specifications of knowingly exceeding authorized access to a government computer, in violation of Articles 92, 104, and 134, Uniform Code of Military Justice (UCMJ) 10 U.S.C. §§ 892, 904, 934 (2010). The case has been referred to a general court martial by the convening authority.
2. The Defense argues the following 4 categories of specifications are an UMC against PFC Manning. The specifications are identified in relevant part:

Category 1: Article 134 (18 U.S.C. 641) and Article 134 (18 U.S.C. 793(e))

(A) Charge II, specifications 4 and 5 involving the Combined Information Data Network Exchange Iraq database containing more than 380,000 records belonging to the United States government:

Specification 4 of Charge II: Article 134 (18 U.S.C. 641) – PFC Manning did at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 5 January 2010, “steal, purloin, or knowingly convert “the Combined Information Data Network Exchange Iraq database containing more than 380,000 records belonging to the United States government,” in violation of 18 U.S.C. Section 641 and Article 134.

Specification 5 of Charge II: Article 134 (18 U.S.C. 793(e))- PFC Manning having unauthorized possession of classified Combined Information Data Network Exchange Iraq database records, did, at the same place specified in Specification 4 between on or about 31 December 2009 and on or about 9 February 2010, willfully communicate, deliver, transmit, or cause to be communicated, delivered or transmitted, these records to a person not entitled to receive them with reason to believe that the records could be used to the injury of the United States or to the advantage of any foreign nation, in violation of 18 U.S.C. Section 793(e) and Article 134.

(B) Charge II, specifications 6 and 7 involving the Combined Information Data Network Exchange Afghanistan database containing more than 90,000 records belonging to the United States government:

Specification 6 of Charge II: Article 134 (18 U.S.C. 641) – PFC Manning did at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 8 January 2010,” steal, purloin, or knowingly convert “the Combined Information Data Network Exchange Afghanistan database containing more than 90,000 records belonging to the United States government,” in violation of Section 641 and Article 134.

Specification 7 of Charge II: Article 134 (18 U.S.C. 793(e)) - PFC Manning did having unauthorized possession of classified records contained on the Combined Information Data Network Exchange Afghanistan database, did, at the same place specified in Specification 6 between on or about 31 December 2009 and on or about 9 February 2010, willfully communicate, deliver, transmit, or cause to be communicated, delivered or transmitted, these records to a person not entitled to receive them with reason to believe that the records could be used to the injury of the United States or to the advantage of any foreign nation, in violation of Section 793(e) and Article 134.

(C) Charge II, specifications 8 and 9 involving the United States Southern Command database containing more than 700 records belonging to the United States government:

Specification 8 of Charge II: Article 134 (18 U.S.C. 641) – PFC Manning did at or near Contingency Operating Station Hammer, Iraq, on or about 8 March 2010,” steal, purloin, or knowingly convert “a United States Southern Command database containing more than 700 records belonging to the United States government,” in violation of Section 641 and Article 134.

Specification 9 of Charge II: Article 134 (18 U.S.C. 793(e)) - PFC Manning having unauthorized possession of classified records contained on the database specified in Specification 8, did, at the same place specified in Specification 8 between on or about 8 March 2010 and on or about 27 May 2010, willfully communicate, deliver, transmit, or cause to be communicated, delivered or transmitted, these records to a person not entitled to receive them with reason to believe that the records could be used to the injury of the United States or to the advantage of any foreign nation, in violation of Section 793(e) and Article 134.

Category 2: Article 134 (18 U.S.C. 641) and 18 U.S.C. 1030(a)(1)

(A) Charge II, specifications 12 and 13 involving the Department of State Net-Centric Diplomacy database containing more than 250,000 records belonging to the United States government:

Specification 12 of Charge II: Article 134 (18 U.S.C. 703(e)) - PFC Manning did at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 4 May 2010," steal, purloin, or knowingly convert "the Department of State Net-Centric Diplomacy database containing more than 250,000 records belonging to the United States government," in violation of Section 641 and Article 134.

Specification 13 of Charge II: Article 134 (18 U.S.C. 1030(a)(1)) - PFC Manning, at the same place specified in Specification 12 between on or about 28 March 2010 and on or about 27 May 2010, knowingly exceeded his authorized access on a Secret Internet Protocol Router computer, obtained classified Department of State cables determined to require protection against unauthorized disclosure, and willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, these cables to a person not entitled to receive them with reason to believe that these cables so obtained could be used to the injury of the United States, in violation of 18 U.S.C. Section 1030(a)(1) and Article 134.

Category 3: Charges Occurring in a single transaction on the same day:

(A) Charge II, specifications 4, 5, 6, and 7.

(B) Charge II, specifications 10 and 11 (18 U.S.C. 793(e)).

Specification 10 of Charge II: Article 134 (18 U.S.C. 793(e)) - PFC Manning, having unauthorized possession of classified records relating to a military operation in Farah Province, Afghanistan occurring on or about 4 May 2009, did, "at or near Contingency Operating Station Hammer, Iraq, between on or about 11 April 2010 and on or about 27 May 2010," willfully communicate, deliver, transmit, or cause to be communicated, delivered or transmitted, these records to a person not entitled to receive them with reason to believe that the records could be used to the injury of the United States or to the advantage of any foreign nation, in violation of Section 793(e) and Article 134.

Specification 11 of Charge II: Article 134 (18 U.S.C. 793(e)) - PFC Manning, having unauthorized possession of a file containing a video relating to the national defense, did, "at or near Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 8 January 2010," willfully communicate, deliver, transmit, or cause to be communicated, delivered or transmitted, this file to a person not entitled to receive it with reason to believe that the file could be used to the injury of the United States or to the advantage of any foreign nation, in violation of Section 793(e) and Article 134.

The Law:

1. RCM 307(c)(4) states that “[w]hat is substantially one transaction should not be made the basis for an unreasonable multiplication of charges against one person.”¹ The central tenet of the doctrine is to “promote fairness considerations separate from an analysis of the statutes, their elements, and the intent of Congress.” *United States v. Quiroz*, 55 M.J. 334, 337 (C.A.A.F. 2001), discussing *United States, v. Teters*, 37 M.J. 370 (CMA 1993).

2. The Court of Appeals for the Armed Forces in *U.S. v. Campbell*, 71 M.J. 19 (C.A.A.F. 2012) endorsed the following non-exclusive factors, commonly known as *Quiroz* factors, as a guide for military judges to consider when the defense objects that the Government has unreasonably multiplied the charges:

- (1) whether each charge and specification aimed at distinctly separate criminal acts?
- (2) whether the number of charges and specifications misrepresent or exaggerate the accused’s criminality?
- (3) whether the number of charges and specifications *unfairly* increase the appellant’s punitive exposure?
- (4) Whether there any evidence of prosecutorial overreaching or abuse in the drafting of the charges?

None of the factors are pre-requisites. One or more factors may be sufficient to establish an UMC based on prosecutorial over-reaching. A singular act may implicate multiple and significant criminal law interests, none necessarily dependent upon the other. UMC may apply differently to findings than to sentencing. A charging scheme may not implicate the *Quiroz* factors in the same way that sentencing exposure does. In such a case, the nature of the harm requires a remedy that focuses more appropriately on punishment than findings. *Campbell*, 71 M.J. 23, 24.

3. The Court must, therefore scrutinize the prosecutor’s charging determinations as “the prohibition against unreasonable multiplication of charges addresses those features of military law that increase the potential for overreaching in the exercise of prosecutorial discretion.” *Id.* The application of the *Quiroz* factors, at bottom, involves a “reasonableness determination, much like sentence appropriateness.” *United States v. Anderson*, 68 M.J. 378, 386 (C.A.A.F. 2010).

4. Where a trial court finds an unreasonable multiplication of charges, dismissal of the multiplied charges is an available remedy. *United States v. Roderick*, 62 M.J. 425, 433 (C.A.A.F. 2006). Consolidation of the unreasonably multiplied charges is also a remedy available to the trial court. *United States v. Gilchrist*, 61 M.J. 785, 789 (A. Ct. Crim. App. 2005).

ANALYSIS:

Category I: The 18 U.S.C. § 641 and 18 U.S.C. § 793(e) Specifications

¹ However, the RCM are not so inflexible as to fail to recognize that situations may arise “when sufficient doubt as to the facts or the law exists to warrant making one transaction the basis for charging two or more offenses.” See discussion to RCM 307(c)(4).

(Specifications 4 & 5, 6 & 7, and 8 & 9, of Charge II)

1. The 18 U.S.C. § 641 and 18 U.S.C. § 793(e) specifications address distinctly separate criminal acts. The 18 U.S.C. § 641 offenses are aimed at the theft of government property, in the present case records contained in government-owned databases, while the gravamen of the 18 U.S.C. § 793(e) offenses is the transmittal of national defense information to unauthorized persons. The distinct nature of the paired specifications is illustrated by comparing the elements of the offenses. See *U.S. v. Pauling*, 60 M.J. 91, 95 (C.A.A.F. 2004) (referring to the court's multiplicity analysis in deciding that the specifications at issue were aimed at distinctly separate criminal acts; charging the forgery of 16 checks and four indorsements in two specifications were aimed at as a fair and reasonable exercise of prosecutorial discretion). In order to prove the accused violated 18 U.S.C. § 641 – Specifications 4, 6, and 8 – the United States must establish that the accused stole, purloined, or knowingly converted United States Government property. In order to prove the accused violated 18 U.S.C. § 793(e) – Specifications 5, 7, and 9 – the United States must establish that the accused communicated, delivered, or transmitted national defense information to a person not entitled to receive it. The Defense argument that each violation of 18 U.S.C. § 641 was simply the “first step” in a violation of 18 U.S.C. § 793(e) has been discounted by the appellate courts in the context of larceny and false claims convictions *United States v. Chatman*, 2003 WL 25945959 (A. Ct. Crim. App. June 13, 2003) (unpublished) (noting that the specific intent to deprive the United States of its military property is a *mens rea* unnecessary for the Article 132 offenses). See also *Campbell* (recognizing that a singular act may implicate multiple and significant criminal interests not dependent on the others). Each specification alleging a violation of 18 U.S.C. § 641 is directed at misconduct wholly independent of its paired specification alleging a violation of 18 U.S.C. § 793(e). As in *Campbell*, in this case, the crime of theft of government records can be complete whether or not the accused willfully “communicated.....transmitted” the records to persons not entitled to receive them.

2. The number of charges and specifications do not misrepresent or exaggerate the accused's criminality. A facial analysis of the charge sheet shows that Specifications 4, 6, 8, and 12 of Charge II allege a theft of government property from four different databases (the Combined Information Data Network Exchange Iraq database, the Combine Information Data Network Exchange Afghanistan database, a United States Southern Command database, and the Department of State Net-Centric Diplomacy database). Moreover, the volume of records alleged to have been stolen augers in favor of the Government (more than 380,000 records; more than 90,000 records; more than 700 records; more than 250,000 records).

3. The number of charges and specifications do not unfairly increase the accused's punitive exposure as an UMC for findings. Charging the accused with knowingly giving intelligence to the enemy, delivering national defense information to those unauthorized to receive it, theft of government property, and conduct prejudicial to good order and discipline, based on the accused's posting of classified information to a publicly accessible website, totaling hundreds of thousands of records, over the span of several months, is not an unreasonable multiplication of charges. The Article 104 offense has a maximum punishment of life confinement without the eligibility for parole. The Government could have broken up the single specification into multiple specifications based on specific Internet postings. See *Campbell*, 71 at 25. The

maximum possible punishment for a conviction under either 18 U.S.C. § 641 or 18 U.S.C. § 793(e) is ten years incarceration for each specification. Therefore, dismissal of Specifications 4, 6, and 8 would reduce the accused's punitive exposure by 30 years. In this case, considering the alleged volume of government and classified records involved, the accused's punitive exposure has not been unfairly increased for purposes of UMC for findings. See *United States v. Anderson*, 68 M.J. 378, 386 (C.A.A.F. 2010).

4. There is no evidence of prosecutorial overreaching or abuse in the drafting of charges. The Defense points to the charge sheet to support its contention that the government is "pil[ing] on the charges against PFC Manning in order to increase the likelihood of a severe sentence if he is convicted." Def. Mot. at 7. As the Court has already found, the charges are distinct in nature and proof and involve voluminous Government records. The Defense argues the Government has pushed 18 U.S.C. § 641 "to the edge of its permissible application" as it relates to national defense information, relying on the separate view expressed by Judge Winter in *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980). This argument has been rejected by the Second, Fourth, and Sixth Circuits. *United States v. Girard*, 601 F.2d 69, 70-71 (2nd Cir. 1979); *United States v. Fowler*, 932 F.2d 306 (4th Cir. 1991); *United States v. Jeter*, 775 F.2d 670, 680-82 (6th Cir. 1985). Even if the Government mischarged the accused with violations of 18 U.S.C. § 641, no relief would be warranted under the theory that the government engaged in UMC.

5. The Government has conceded that the transmissions in specifications 5 and 7 were one transmission, although of voluminous records. The Court will leave those specifications as separate charges until after findings are announced. The Defense may make a motion to merge the specifications for findings at that time.

**Category II: 18 U.S.C. § 641 and 18 U.S.C. § 1030(a)(1)
(Specifications 12 & 13 of Charge II)**

1. The 18 U.S.C. § 641 and 18 U.S.C. § 1030(a)(1) specifications encompass distinctly separate criminal acts. The 18 U.S.C. § 641 offense is aimed at the theft of government property, in the present case records contained in government-owned databases, while the 18 U.S.C. § 1030(a)(1) offense requires the transmittal of classified information to unauthorized persons. The same rationale of paragraph (1) in Category I also applies to these offenses. The specification alleging a violation of 18 U.S.C. § 641 is directed at misconduct wholly independent of its paired specification alleging a violation of 18 U.S.C. § 1030(a)(1).

2. The number of charges and specifications do not misrepresent or exaggerate the accused's criminality. A singular act may implicate multiple and significant criminal law interests, none necessarily dependent upon the other. In this case, the crime of theft of government records can be complete whether or not the accused willfully "communicated.....transmitted" the records to persons not entitled to receive them. The decision by the Government to charge the accused with theft of government property and exceeding authorized access on a computer and with transmitting classified information is a reasonable exercise of prosecutorial discretion.

3. The Court finds the number of charges and specifications do not unfairly increase the accused's punitive exposure for purposes of UMC for findings. Charging the accused with knowingly giving intelligence to the enemy, delivering national defense information to those unauthorized to receive it, theft of government property, and conduct prejudicial to good order and discipline, based on the accused's posting of classified information to a publicly accessible website, totaling hundreds of thousands of records, over the span of several months, is not an unreasonable multiplication of charges. The Article 104 offense has a maximum punishment of life confinement without the eligibility for parole. The Government could have broken up the single specification into multiple specifications based on specific Internet postings. Dismissal of Specification 12 would reduce the accused's punitive exposure by 10 years. Based on all of the above, the accused's punitive exposure has not been *unfairly* increased for purposes of UMC for findings. See *United States v. Anderson*, 68 M.J. 378, 386 (C.A.A.F. 2010).

4. There is no evidence of prosecutorial overreaching or abuse in the drafting of charges for the reasons set forth in paragraphs 1-3 above.

**Category 3: Specifications Directed at Conduct That Occurred on the Same Day
(Specifications 4, 5, 6 & 7 of Charge II)
(Specifications 10 & 11 of Charge II)**

1. The Defense concedes there is a factual dispute whether the conduct in specifications 10 and 11 of Charge II occurred on the same day or not.

2. The parties dispute whether the conduct at issue in specifications 4, 5, 6, and 7 of Charge II occurred on the same or separate days. Whether the enumerated specifications are directed at conduct that occurred on one day or different days is a factual matter that should be determined by the fact-finder after the close of the evidence. The Defense may re-raise this UMC motion after findings have been announced.

RULING: The Defense Motion to Dismiss Based on Unreasonable Multiplication of Charges for Findings is **DENIED**.

The Defense may re-raise the Motion to Dismiss for UMC for Findings and/or Sentence after announcement of the findings.

So ORDERED this 25th day of April 2012.



DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit

KEY PROVISIONS FROM AR 380-5

Section VII

Corrective Actions and Sanctions

1-20. General

Commanders will establish procedures to make sure that prompt and appropriate action is taken concerning a violation of the provisions of this regulation, especially in those cases involving incidents which can put classified information at risk of compromise, unauthorized disclosure, or improper classification of information. Such actions will focus on a correction or elimination of the conditions that caused or contributed to the incident.

1-21. Sanctions

a. DA personnel will be subject to sanctions if they knowingly, willfully, or negligently—

- (1) Disclose classified or sensitive information to unauthorized persons.
- (2) Classify or continue the classification of information in violation of this regulation.
- (3) Violate any other provision of this regulation.

b. Sanctions can include, but are not limited to warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and removal of original classification authority. Action can also be taken under the Uniform Code of Military Justice (UCMJ) for violations of that Code and under applicable criminal law, if warranted.

c. Original classification authority will be withdrawn for individuals who demonstrate a disregard or pattern of error in applying the classification and sensitivity standards of this regulation.

Section V

Sensitive Information (Computer Security Act of 1987)

5-19. Description

a. The Computer Security Act of 1987 established requirements for protection of certain information in federal government Automated Information Systems (AIS). This information is referred to as "sensitive" information, defined in the Act as: "Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, USC (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

b. Two aspects of this definition deserve attention. First, the Computer Security Act of 1987 applies only to unclassified information which deserves protection. Second, unlike most other programs for protection of information, the Computer Security Act of 1987 is concerned with protecting the availability and integrity, as well as, the confidentiality of information. Much of the information which fits the Computer Security Act of 1987's definition of "sensitive" falls within the other categories of information discussed in this chapter.

3.0. Definitions

3.1. "Caveated" information is information subject to one of the authorized control markings under section 9.

3.2. Intelligence Community (and agencies within the Intelligence Community) refers to the United States Government agencies and organizations and activities identified in section 3 of the National Security Act of 1947, as amended, 50 USC 401a(4), and section 3.4(f) (1 through 6) of Executive Order 12333.

3.3. Intelligence information and related materials (hereinafter referred to as "Intelligence") include the following information, whether written or in any other medium, classified pursuant to EO 12958 or any predecessor or successor Executive Order.

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army, xxx-xx-)

Headquarters and Headquarters Company,)

U.S. Army Garrison, Joint Base Myer-)

Henderson Hall, Fort Myer, VA 22211)

**RULING: DEFENSE MOTION
TO DISMISS SPECIFICATION I
OF CHARGE II FOR FAILURE
TO STATE AN OFFENSE**

DATED: 25 April 2012

Defense moves the Court to dismiss Specification I of Charge II for failure to state a cognizable offense under Article 134 because it is preempted by Article 134, or, in the alternative, that the specification must be charged as a violation of Article 92. Government opposes. After considering the pleadings, evidence presented, and argument of counsel, the Court finds and concludes the following:

Factual Findings:

1. Specification 1 of Charge I alleges that PFC Manning "between on or about 1 November 2009 and on or about 27 May 2010, without proper authority knowingly gave intelligence to the enemy, through indirect means" in violation of Article 104, UCMJ.
2. Specification 1 of Charge II, alleges that PFC Manning "wrongfully and wantonly caused to be published on the internet intelligence belonging to the United States government, having knowledge that intelligence published on the internet is accessible to the enemy, such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces" in violation of Article 134, UCMJ.
3. At the time of PFC Manning's alleged unlawful actions, Army Regulation 380-5 (Department of the Army Information Security Program) was in effect. The regulation is a punitive lawful general order per paragraph 1-21 which states the following:

1-21. Sanctions

- a. DA personnel will be subject to sanctions if they knowingly, willfully, or negligently -

- (1) Disclose classified or sensitive information to unauthorized persons.

- (2) Classify or continue the classification of information in violation of this

regulation.

- (3) Violate any other provision of this regulation.

- b. Sanctions can include, but are not limited to warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and removal of original classification authority. Action can also be taken under the Uniform Code of Military Justice for violations of that Code and under applicable criminal law, if warranted. .

4. AR 380-5 defines classified information as “information and material that has been determined, pursuant to EO 12958 or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary and readable form. Sensitive information but unclassified information is defined as “information originated from within the Department of State which warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the Freedom of Information Act.” Sensitive Compartmentalized Information is defined as “classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

5. Intelligence is defined under Article 104c(4) as information that may be useful to the enemy for any of the many reasons that make information valuable to belligerents. Intelligence imports that the information conveyed is true or implies the truth, at least in part.

The Law - Preemption:

1. The preemption doctrine is explained in paragraph 60(c)(5)(a) of the Manual for Courts-Martial (MCM), which provides, in pertinent part:

The preemption doctrine prohibits application of Article 134 to conduct covered by Articles 80 through 132. For example, larceny is covered in Article 121, and if an element of that offense is lacking – for example, intent – there can be no larceny or larceny-type offense, either under Article 121 or, because of preemption, under Article 134. Article 134 cannot be used to create a new kind of larceny offense, one without the required intent, where Congress has already set the minimum requirements for such an offense in Article 121.

MCM, para. 60(c)(5)(a).

2. In *United States v. Kick*, 7 M.J. 82, 85 (C.M.A. 1979), the then Court of Military Appeals (CoMA) stated that the doctrine of preemption is defined as “the legal concept that where Congress has occupied the field of a given type of misconduct by addressing it in one of the specific punitive articles of the code, another offense may not be created and punished under Article 134, UCMJ, simply by deleting a vital element.” The CoMA also stated, “However, simply because the offense charged under Article 134, UCMJ, embraces all but one element of an offense under another article does not trigger the preemption doctrine. *Id.*”

3. Military appellate courts apply a two-pronged test to determine whether an Article 134 charge is preempted by another Article. Both prongs must be met for preemption to apply. First, it must be established that Congress “indicate[d] through direct legislative language or express legislative history that particular actions or facts are limited to the express language of an enumerated article, and may not be charged under Article 134, UCMJ.” *United States v. Anderson*, 68 M.J. 378, 387 (C.A.A.F. 2010); see *Kick*, 7 M.J. at 85; *United States v. Wright*, 5 M.J. 106, 110-11 (C.M.A. 1978). Second, it must be shown that the offense charged under

Article 134 is composed of a "residuum of elements" of an enumerated offense under the UCMJ. *Wright*, 5 M.J. at 111;

4. Military courts are "extremely reluctant to conclude that Congress intended [] provisions to preempt [an] offense...in the absence of a clear showing of a contrary intent." The fact that an Article 134 offense embraces all but one element of an offense under an enumerated article does not trigger the preemption doctrine. See *Kick*, 7 M.J. at 85.

5. The issue of whether Congress indicated through direct legislative language or express legislative history that Article 104 cover a class of offenses in a complete way addressed by the Court of Appeals for the Armed Forces (CAAF) in *Anderson*. In that case the Government charged the accused with violating Articles 80 and 104, UCMJ by knowingly giving intelligence to the enemy and two specifications of attempting to communicate with the enemy. The accused was also charge with violating Article 134, UCMJ, by wrongfully and dishonorably providing information on U.S. Army troop movements to persons whom the accused thought were Tariq Hamdi and Mohammed, members of the al Qaida terrorist network, such conduct being prejudicial to good order and discipline in the armed forces, and of a nature to bring discredit upon the armed forces. CAAF applied the two-part preemption test and concluded Article 104 did not preempt an Article 134 offense for distributing sensitive material to individuals not authorized to receive it. First, the CAAF concluded that "the legislative history of Article 104 does not clearly indicate that Congress intended for offenses similar to those at issue [i.e., the distribution of sensitive material to individuals not authorized to receive it] to only be punishable under Article 104 to the exclusion of Article 134." Therefore, the CAAF concluded that the Article 104 and Article 134 offenses may encompass parallel facts but the charged offenses are directed at distinct conduct.

Analysis: Preemption

1. Despite the Defense's attempt to distinguish this case from *Anderson*, the facts of *Anderson* are sufficiently similar to prove controlling. The CAAF in *Anderson* concluded Article 104 did not preempt an Article 134 offense for distributing sensitive material to individuals not authorized to receive it. The accused in *Anderson* provided undercover FBI agents, posing as al Qaeda operatives, computer diskettes containing classified information on the vulnerabilities of military operations. The accused was convicted of attempting to give intelligence to the enemy, attempting to aid the enemy, and conduct prejudicial to good order and discipline.

2. In applying the two-part preemption test in this case, the Court finds that the charged offense of Article 134, UCMJ, in Specification 1 of Charge II, is not preempted by Article 104, UCMJ. Prong 1 of the 2 part test is not met. There is no direct legislative language or express legislative history to show that Congress demonstrated its intent that Article 104 "to cover a class of offenses in a complete way."

3. In applying prong 2 of the test, the charged Article 134 offense is not composed of a residuum of elements of the Article 104 offense. Each offense requires a different *mens rea*. The Article 134 offense requires that the accused "wantonly" caused to be published intelligence belonging to the United States government on the Internet. The Article 104 offense requires the

Government to prove the accused “knowingly” gave intelligence to the enemy and that the enemy received it. The Article 134 offense requires the Government to show that the accused “wantonly” published intelligence on the internet knowing that such intelligence is accessible to the enemy. “Wanton” is not a residuum of “knowing”. The Article 134 offense punishes the wanton publication of intelligence on the internet not giving intelligence to the enemy.

4. Article 104 does not preempt the Article 134 offense charged in specification 1 of Charge II.

The Law – Article 92:

1. Article 134, UCMJ, provides in full as follows:

Though not specifically mentioned in this chapter, all disorders and neglects to the prejudice of good order and discipline in the armed forces, all conduct of a nature to bring discredit upon the armed forces, and crimes and offenses not capital, of which persons subject to this chapter may be guilty, shall be taken cognizance of by a general, special, or summary court-martial, according to the nature and degree of the offense, and shall be punished at the discretion of that court.

2. Violations of customs of the service that are made punishable in punitive regulations should be charged under Article 92 as violations of the regulations in which they appear. No custom may be contrary to existing law or regulation. Explanation to Article 134, Part IV, paragraph 60, c(2)(B).

3. Article 92, UCMJ, provides for punishment of any person subject to the UCMJ who “(1) violates or fails to obey any lawful general order or regulation; (2) having knowledge of any other lawful order issued by a member of the armed forces, which it is his duty to obey, fails to obey the order; or (3) is derelict in the performance of his duties[.]” *Id.* § 892

4. In *United States v. Borunda*, 67 M.J. 607 (AF. Ct. Crim. App. 2009), the Air Force Court of Criminal Appeals (AFCCA) stated that possession of drug paraphernalia must be charged under Article 92 rather than Article 134 where a punitive regulation proscribes the conduct. *Citing United States v. Caballero*, 49 C.M.R. 594 (C.M.A. 1975), AFCCA upheld the use of Article 134 to prosecute the appellant for possession of drug paraphernalia where no lawful general order or regulation proscribed such possession, concluding that “in the absence of a lawful general order or regulation, charging officials are at liberty to charge the possession of drug paraphernalia as a violation of Article 92(3), UCMJ, or Article 134, UCMJ.”

Analysis:

1. If AR 380-5, paragraph 1-21 is not punitive, then there is no issue whether specification 1 of Charge II is properly charged under Article 92 or 134. The Court assumes for the purposes of this motion that AR 380-5, paragraph 1-21 is punitive.

2. Specification 1 of Charge II, charges the accused with wrongfully and wantonly causing to be published on the internet intelligence belonging to the United States government, having knowledge that intelligence published on the internet is accessible to the enemy, such intelligence being prejudicial to good order and discipline and of a nature to bring discredit upon the armed force. The conduct at issue in specification charged Article 134 offense is distinct from an Article 92 offense under AR 380-5, para. 1-21a. AR 380-5 punishes knowing, willful, or negligent disclosure of classified or sensitive information to unauthorized persons. It does not punish the "wanton" conduct charged in specification 1 of Charge II and intelligence encompasses more than classified and sensitive information.

3. The question in this case is whether the existence of a punitive regulation governing information security that punishes knowing, willful, and negligent disclosures of classified information to unauthorized persons precludes the Government from charging an offense under Article 134 that includes a wanton *mens rea*, adds an additional element not included in the AR 380-5 offense, that the accused knew that intelligence published on the internet is accessible to the enemy, and punishes the distribution of "intelligence" which includes information that does not fall within AR 380-5, where the conduct charged under Article 134 is prejudicial to good order and discipline in the armed forces or service discrediting.

4. The Court finds that the fact that there is a punitive regulation governing the Army Information Security Program, AR 380-5, that does not proscribe the conduct charged in specification 1 of Charge II, wrongful and wanton publication of intelligence on the internet knowing that such intelligence is accessible to the enemy, where such conduct is prejudicial to good order and discipline or service discrediting does not preclude the charge under Article 134. This case is distinct from *Borunda*, as that case addressed an Article 134 specification where the offense charged was specifically proscribed in a punitive regulation. Because the conduct charged in specification 1 of Charge II is not specifically proscribed by AR 380-5, the Government is "at legal liberty to charge the offense as a violation of Article 92(3) or Article 134." *Borunda*, 67 M.J. at 609-10.

RULING: The Defense Motion to dismiss Specification 1 of Charge II for preemption and failure to state a cognizable offense under Article 134 is **DENIED**.

So **ORDERED**: this 25th day of April 2012.



DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, xxx-xx-██████

HHC, U.S. Army Garrison

Joint Base Myer-Henderson Hall

Fort Myer, Virginia 22211

**RULING: DEFENSE MOTION
TO DISMISS FOR FAILURE TO
STATE AN OFFENSE**

DATED: 26 April 2012

Defense moves this Court to dismiss the Specification of Charge I for failure to state an offense. Alternatively, Defense moves to dismiss the Specification of Charge I because the inclusion of the term “indirectly” in Article 104, UCMJ, renders that provision unconstitutionally vague and substantially overbroad. Government opposes. The Government moves the Court to adopt the instructions for Article 104(2) (Giving Intelligence to the Enemy) in *Department of the Army Pamphlet, 27-9, Military Judge’s Benchbook* (Benchbook). After considering the pleadings, evidence presented, and argument of counsel, the Court finds and concludes the following:

Factual Findings:

1. The Government provided particulars regarding the specification of Charge I in response to the Defense question, “How did PFC Manning knowingly give intelligence to the enemy?” The Government responded “PFC Manning knowingly gave intelligence to the enemy by transmitting certain intelligence, specified in a separate classified document, to the enemy through the WikiLeaks website.”
2. In the specification of Charge I, the accused is charged with Giving Intelligence to the Enemy in violation of Article 104(2). The specification alleges that between on or about 1 November 2009 and on or about 27 May 2010, PFC Manning, without proper authority, knowingly gave intelligence to the enemy through indirect means. The specification follows the model specification in the Manual for Courts Martial (MCM) Part IV, paragraph 28(f)(3)(Article 104-Aiding the Enemy – Giving Intelligence to the Enemy).

The Law: Article 104

1. Article 104(2) makes it a crime for “any person who, without proper authority, knowingly harbors or protects or gives intelligence to or communicates or corresponds with or holds any intercourse with the enemy, either directly or indirectly.”
2. Article 104b(4) provides the following elements for the offense of Giving Intelligence to the Enemy:

(a) that the accused, without proper authority, knowingly gave intelligence information to the enemy, and;

(b) that the intelligence information was true or implied the truth, at least in part.

In addition, MCM Part IV, Paragraph 28b(5)(a)-(c) provide the following explanation:

(a) *Nature of offense*: Giving intelligence to the enemy is a particular case of corresponding with the enemy made more serious by the fact that the communication contains intelligence that may be useful to the enemy for any of the many reasons that make information valuable to belligerents. This intelligence may be conveyed by direct or indirect means.

(b) *Intelligence*: “Intelligence” imports that the information conveyed is true or implies the truth, at least in part.

(c) *Knowledge*: Actual knowledge is required but may be proved by circumstantial evidence.

3. Giving Intelligence to the Enemy under Article 104(2) requires actual knowledge by the accused that he was giving intelligence to the enemy. MCM, Paragraph 28c(5(c)). This is true whether the giving of intelligence is by direct or indirect means. A person cannot violate Article 104 by acting inadvertently, accidentally, or negligently. *U.S. v. Olson*, 20 C.M.R. 461 (A.B.R. 1955).

4. The Military Judge’s Benchbook provides instructions for Article 104(2)(3-28-4). Those instructions do not include instructions defining “knowledge” or “indirect means”.

The Law: Failure to State an Offense.

The military is a notice pleading jurisdiction. A charge and its specification is sufficient if it (1) contains the elements of the offense charged and fairly informs an accused of the charge against which he must defend; and (2) enables the accused to plead an acquittal or conviction in bar of future prosecutions for the same offense. *U.S. v. Fosler*, 70 M.J. 225 (C.A.A.F. 2011). A motion to dismiss for failure to state an offense is a challenge to the adequacy of a specification and whether the specification “alleges, either expressly or by implication, every element of the offense, so as to give the accused notice and protection against double jeopardy.” *United States v. Amazaki*, 67 M.J. 666, 669, 670 n.8 (A. Ct. Crim. App. 2009) (quoting *United States v. Crafter*, 64 M.J. 209, 211 (C.A.A.F. 2006)).

The Law: Void for Vagueness.

1. A motion to dismiss a specification as being “void for vagueness” implicates the Due Process clause of the Fifth Amendment. To overcome a “void for vagueness challenge”, a statute must be reasonably clear so as to provide warning of the type of conduct which is proscribed and provide standards sufficiently explicit to prevent arbitrary and capricious application. A statute

is impermissibly vague if it “(1) fails to provide people of ordinary intelligence a reasonable opportunity to understand what conduct it prohibits; or (2) authorizes or even encourages arbitrary and discriminatory enforcement.” *U.S. v. Shrader*, 2012 WL 1111654 (4th Circuit, 4 April 2012) *quoting* *Hill v. Colorado*, 530 U.S. 703, 732 (2000); *U.S. v. Amasaki*, 67 M.J.666 (Army Ct. Crim. App. 2009). “[T]he more important aspect of vagueness doctrine is not actual notice, but the other principal element of the doctrine—the requirement that a legislature establish minimal guidelines to govern law enforcement.” Courts also consider any judicial or administrative limiting construction of a criminal statute in determining whether it is unconstitutionally vague. *Kolendar v. Lawson*, 461 U.S. 352, 355, 357, 358 (1983).

2. A “knowing” scienter requirement mitigates a law’s vagueness especially with respect to actual notice of the conduct proscribed. *U.S. v. Moyer*, 2012 WL 639277 (3rd Cir. 2012).

The Law: Substantially Overbroad.

1. A statute is facially overbroad when no set of circumstances exists under which it would be valid. *United States v. Salerno*, 481 U.S. 739, 745 (1987). The Defense does not challenge Article 104(2) as facially overbroad.

2. In the First Amendment context, a statute is “overbroad” when a substantial number of its applications are unconstitutional when compared with the statute’s plainly legitimate sweep. *U.S. v. Stevens*, 130 S. Ct. 1577 (2010).

Conclusions of Law: Failure to State an offense.

1. The general intent required by Article 104 is knowledge. This general intent is alleged in the specification.

2. Knowledge is a recognized *mens rea* to provide an evil state of mind. *U.S. v. Morrisette*, 342 U.S. 246 (1952) (holding that “mere omission from 18 U.S.C. 641 of any mention of intent will not be construed as eliminating that element from the crimes denounced” and distinguishing between crimes requiring guilty knowledge/*mens rea* from strict liability offenses).

3. The Defense in paragraph 13 of its brief argues “knowing” is an insufficient *mens rea* and states that “It is clear that in order to state an offense under Article 104(2) the Government must allege that PFC Manning *intended* to give intelligence to the enemy.” “Knowingly” is an evil mind *mens rea*. Article 104(2) does not require a specific intent or motive to give intelligence to the enemy.

4. The Government bill of particulars response to the question “How did PFC Manning knowingly give intelligence to the enemy?” that “PFC Manning knowingly gave intelligence to the enemy by transmitting certain intelligence, specified in a separate classified document, to the enemy through the WikiLeaks website.” does not impact on whether the specification states an offense. The Bill of Particulars response states that the Government is prepared to prove the accused had actual knowledge he was giving intelligence to the enemy.

5. The specification of Charge I includes all of the elements of the offense, fairly informs the accused of the charge against which he must defend, and protects the accused against double jeopardy.

6. The specification of Charge I states an offense.

7. That said, the Government requests the Court to adopt the instructions for Article 104(2) Giving Intelligence to the Enemy that are in the *Military Judge's Benchbook*. The Court will give the instructions in the *Benchbook* but notes that there is no "knowledge" instruction or instruction of what is meant by "indirect means". The Court proposes to give a knowledge instruction along the lines of the following:

"Knowingly means Giving Intelligence to the Enemy under Article 104(2) requires actual knowledge by the accused that he was giving intelligence to the enemy. This is true whether the giving of intelligence is by direct or indirect means. A person cannot violate Article 104 by acting inadvertently, accidentally, or negligently." See MCM, Paragraph 28c(5)(c)). *U.S. v. Olson*, 20 C.M.R. 461 (A.B.R. 1955).

The Court proposes to give an instruction on "indirect means" along the lines of the following:

"Indirect means" means that the accused knowingly gave the intelligence to the enemy through a 3rd party or in some other indirect way. The accused must actually know that by giving the intelligence to the 3rd party that he was giving intelligence to the enemy through this indirect means."

The Court invites the parties to propose "knowledge" and "indirect means" instructions.

Conclusions of Law: Void for Vagueness – Term Indirectly.

1. The offense of aiding the enemy is not a new or novel offense. *United States v. Olson*, 22 C.M.R. 250, 256, (C.M.A. 1957) ("The offense of aiding . . . the enemy or . . . giving . . . him intelligence is almost as old as warfare itself, and traces of what is clearly the conceptual forefather of . . . Article 104 of the Code may be found in the earliest of recorded military codes."); *U.S. v. Batchelor*, 22 C.M.R. 144 (1956) (aiding the enemy has been an offense in every military code since The American Articles of War in 1775).

2. The Defense argues that the Government's theory is that no criminal intent is required and that a person can violate Article 104(2) by disclosing information on the internet that might be accessible to the enemy. This is not consistent with the Government response in its Bill of Particulars.

3. The term "indirect means" describes the means by which a person knowingly gives intelligence to the enemy. The actual knowledge *mens rea* is the same whether the means of giving the intelligence is direct or indirect. The hypotheticals posed by the defense do not violate Article 104(2) because the person did not have actual knowledge that he/she was giving intelligence to the enemy by indirect means.

4. A Soldier of ordinary intelligence would be on notice that transmitting intelligence specified in a classified document to a website, without authority, with actual knowledge that the enemy used that website is prohibited conduct. The elements that the accused was acting without authority and the *mens rea* requirement of actual knowledge by the accused that he or she is giving intelligence to the enemy, does not encourage arbitrary and discriminatory enforcement of the statute.

5. The specification of Charge I (Giving Intelligence to the Enemy by Indirect Means) is not unconstitutionally vague. The Court will give instructions defining "actual knowledge" and "indirect means".

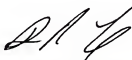
Conclusions of Law: Substantially Overbroad in Violation of the 1st Amendment.

The defense argues that Article 104(2) as charged in the specification of Charge I is substantially overbroad in violation of the 1st Amendment because persons making public statements would be subject to prosecution if the enemy could access it in some form. For the reasons set forth above, the Court finds that Article 104(2) (Giving Intelligence to the Enemy) requires an accused to act without authority, to have actual knowledge that he or she was giving intelligence to the enemy, whether the giving is by direct or indirect means. These elements ensure that Article 104(2)(Giving Intelligence to the Enemy) is not unconstitutionally overbroad and would not prohibit a substantial amount of Constitutionally protected speech.

Conclusion. The specification of Charge I states an offense and is Constitutional. The Court will provide appropriate instructions to fully inform the fact-finder of the elements of the offense and the definitions of "actual knowledge" and "indirect means". If, at trial, the Government does not prove the accused knew that by giving intelligence by indirect means, he actually knew he was giving intelligence to the enemy, the Court will entertain appropriate motions.

RULING: Defense Motion to Dismiss the specification of Charge I is **DENIED**. The Court will adopt the *Benchbook* instructions for Article 104(2) and supplement them with additional instructions regarding actual knowledge and indirect means.

ORDERED, this the 25th day of April 2012.



DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

Section III
Disclosure

23 April 2012

1. In abundance of caution and to ensure the United States provides as much notice as possible to the accused pursuant to Section III of the Military Rules of Evidence (MRE), the United States is operating under the constraints as listed in the United States' Section III disclosure, dated 21 February 2012.
2. Pursuant to MRE 301(c)(2), the United States has not granted or promised immunity or leniency to any witness in this case in exchange for their testimony.
3. Pursuant to MRE 304(d), the United States makes the following updated disclosure of statements, oral and written, made by the accused that are relevant to the case, known to the trial counsel, and within the control of the Armed Forces:

See Enclosure 1.
4. Pursuant to MRE 311(d), the United States is not in possession of any new evidence seized from the person or property of the accused, or believed to be owned by the accused, that it intends to offer into evidence against the accused at trial.
5. Pursuant to MRE 321(c), the United States is not aware of any evidence of a prior eyewitness identification of the accused as a lineup or other identification process that it intends to offer into evidence against the accused at trial.
6. The United States will notify the defense of any updates to paragraphs 2, 3, 4, and 5, as they become known.


ASHDEN FEIN
MAJ, JA
Trial Counsel

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

Section III
Disclosure

Enclosure 1

23 April 2012

BATES # Beginning	BATES # End	Date Produced to Defense
ManningB 00411373	ManningB 00411373	13-Mar-12
ManningB 00412430	ManningB 00412499	13-Mar-12
ManningB 00412538	ManningB 00412545	13-Mar-12
ManningB 00412553	ManningB 00412588	13-Mar-12
ManningB 00412589	ManningB 00412590	13-Mar-12
ManningB 00412591	ManningB 00412592	13-Mar-12
ManningB 00412593	ManningB 00412595	13-Mar-12
ManningB 00412596	ManningB 00412597	13-Mar-12
ManningB 00412598	ManningB 00412599	13-Mar-12
ManningB 00412600	ManningB 00412600	13-Mar-12
ManningB 00412601	ManningB 00412607	13-Mar-12
ManningB 00412608	ManningB 00412608	13-Mar-12
ManningB 00412609	ManningB 00412609	13-Mar-12
ManningB 00412610	ManningB 00412610	13-Mar-12
ManningB 00412611	ManningB 00412611	13-Mar-12
ManningB 00412614	ManningB 00412619	16-Mar-12
ManningB 00412620	ManningB 00412782	16-Mar-12
ManningB 00412783	ManningB 00412783	16-Mar-12
ManningB 00412784	ManningB 00412785	16-Mar-12
ManningB 00412786	ManningB 00412791	16-Mar-12
ManningB 00412792	ManningB 00412795	16-Mar-12
ManningB 00412796	ManningB 00412799	16-Mar-12
ManningB 00412800	ManningB 00412803	16-Mar-12
ManningB 00412804	ManningB 00412807	16-Mar-12
ManningB 00412808	ManningB 00412811	16-Mar-12
ManningB 00412812	ManningB 00412815	16-Mar-12
ManningB 00412816	ManningB 00412819	16-Mar-12
ManningB 00412820	ManningB 00412823	16-Mar-12
ManningB 00412824	ManningB 00412827	16-Mar-12
ManningB 00412828	ManningB 00412829	16-Mar-12
ManningB 00412830	ManningB 00412831	16-Mar-12
ManningB 00412832	ManningB 00412833	16-Mar-12

ManningB 00412834	ManningB 00412835	16-Mar-12
ManningB 00412836	ManningB 00412836	16-Mar-12
ManningB 00412837	ManningB 00412837	16-Mar-12
ManningB 00412838	ManningB 00412838	16-Mar-12
ManningB 00412839	ManningB 00412839	16-Mar-12
ManningB 00412840	ManningB 00412840	16-Mar-12
ManningB 00412841	ManningB 00412841	16-Mar-12
ManningB 00412842	ManningB 00412842	16-Mar-12
ManningB 00412843	ManningB 00412843	16-Mar-12
ManningB 00412844	ManningB 00412844	16-Mar-12
ManningB 00412845	ManningB 00412845	16-Mar-12
ManningB 00412846	ManningB 00412846	16-Mar-12
ManningB 00412847	ManningB 00412853	16-Mar-12
ManningB 00412854	ManningB 00412856	16-Mar-12
ManningB 00412857	ManningB 00412864	16-Mar-12
ManningB 00412865	ManningB 00412868	16-Mar-12
ManningB 00412869	ManningB 00412872	16-Mar-12
ManningB 00412873	ManningB 00412876	16-Mar-12
ManningB 00412877	ManningB 00412880	16-Mar-12
ManningB 00412881	ManningB 00412884	16-Mar-12
ManningB 00412885	ManningB 00412888	16-Mar-12
ManningB 00412889	ManningB 00412892	16-Mar-12
ManningB 00412893	ManningB 00412896	16-Mar-12
ManningB 00412897	ManningB 00412900	16-Mar-12
ManningB 00412901	ManningB 00412904	16-Mar-12
ManningB 00412905	ManningB 00412908	16-Mar-12
ManningB 00412909	ManningB 00412912	16-Mar-12
ManningB 00412913	ManningB 00412916	16-Mar-12
ManningB 00412917	ManningB 00412917	16-Mar-12
ManningB 00412918	ManningB 00412919	16-Mar-12
ManningB 00412920	ManningB 00412921	16-Mar-12
ManningB 00412922	ManningB 00412923	16-Mar-12
ManningB 00412924	ManningB 00412925	16-Mar-12
ManningB 00412926	ManningB 00412927	16-Mar-12
ManningB 00412928	ManningB 00412929	16-Mar-12
ManningB 00412930	ManningB 00412930	16-Mar-12
ManningB 00412931	ManningB 00412931	16-Mar-12
ManningB 00412932	ManningB 00412932	16-Mar-12
ManningB 00412933	ManningB 00412933	16-Mar-12
ManningB 00412934	ManningB 00412934	16-Mar-12
ManningB 00412935	ManningB 00412935	16-Mar-12
ManningB 00412936	ManningB 00412936	16-Mar-12
ManningB 00412937	ManningB 00412937	16-Mar-12

ManningB 00412938	ManningB 00412938	16-Mar-12
ManningB 00412939	ManningB 00412939	16-Mar-12
ManningB 00412940	ManningB 00412940	16-Mar-12
ManningB 00412941	ManningB 00412950	16-Mar-12
ManningB 00412951	ManningB 00412951	16-Mar-12
ManningB 00412952	ManningB 00412952	16-Mar-12
ManningB 00412953	ManningB 00412953	16-Mar-12
ManningB 00412954	ManningB 00412954	16-Mar-12
ManningB 00412955	ManningB 00412955	16-Mar-12
ManningB 00412956	ManningB 00412956	16-Mar-12
ManningB 00412957	ManningB 00412957	16-Mar-12
ManningB 00412958	ManningB 00412962	16-Mar-12
ManningB 00412963	ManningB 00412966	16-Mar-12
ManningB 00412967	ManningB 00412967	16-Mar-12
ManningB 00412968	ManningB 00412974	16-Mar-12
ManningB 00412975	ManningB 00412980	16-Mar-12
ManningB 00412981	ManningB 00412987	16-Mar-12
ManningB 00412988	ManningB 00412992	16-Mar-12
ManningB 00412993	ManningB 00412999	16-Mar-12
ManningB 00413000	ManningB 00413006	16-Mar-12
ManningB 00413007	ManningB 00413013	16-Mar-12
ManningB 00413014	ManningB 00413014	16-Mar-12
ManningB 00413015	ManningB 00413015	16-Mar-12
ManningB 00413016	ManningB 00413016	16-Mar-12
ManningB 00413017	ManningB 00413017	16-Mar-12
ManningB 00413026	ManningB 00413796	16-Mar-12
ManningB 00417536	ManningB 00417539	16-Mar-12
ManningB 00417540	ManningB 00417543	16-Mar-12
ManningB 00417552	ManningB 00417553	16-Mar-12
ManningB 00417554	ManningB 00417557	16-Mar-12
ManningB 00417558	ManningB 00417560	16-Mar-12
ManningB 00417561	ManningB 00417564	16-Mar-12
ManningB 00417572	ManningB 00417581	16-Mar-12
ManningB 00417703	ManningB 00417707	16-Mar-12
ManningB 00417708	ManningB 00417711	16-Mar-12
ManningB 00417774	ManningB 00417784	16-Mar-12
ManningB 00417791	ManningB 00417792	16-Mar-12
ManningB 00417796	ManningB 00417796	16-Mar-12
ManningB 00417797	ManningB 00417797	16-Mar-12
ManningB 00417798	ManningB 00417812	16-Mar-12
ManningB 00417820	ManningB 00417826	16-Mar-12
ManningB 00417827	ManningB 00417835	16-Mar-12
ManningB 00417836	ManningB 00417842	16-Mar-12

ManningB 00418562	ManningB 00418574	12-Apr-12
ManningB 00418690	ManningB 00418744	12-Apr-12
ManningB 00418745	ManningB 00418915	12-Apr-12
ManningB 00418916	ManningB 00418989	12-Apr-12
ManningB 00418990	ManningB 00418994	12-Apr-12
ManningB 00419065	ManningB 00419066	12-Apr-12
ManningB 00419099	ManningB 00419103	12-Apr-12
ManningB 00419104	ManningB 00419117	12-Apr-12
ManningB 00419118	ManningB 00419122	12-Apr-12
ManningB 00419136	ManningB 00419138	12-Apr-12
ManningB 00419139	ManningB 00419220	12-Apr-12
ManningB 00419221	ManningB 00419236	12-Apr-12
ManningB 00419253	ManningB 00419258	12-Apr-12
ManningB 00419471	ManningB 00419471	12-Apr-12
ManningB 00419472	ManningB 00419472	12-Apr-12
ManningB 00419473	ManningB 00419486	12-Apr-12
ManningB 00419487	ManningB 00419487	12-Apr-12
ManningB 00419488	ManningB 00419493	12-Apr-12
ManningB 00419494	ManningB 00419494	12-Apr-12
ManningB 00419495	ManningB 00419495	12-Apr-12
ManningB 00419496	ManningB 00419496	12-Apr-12
ManningB 00419497	ManningB 00419502	12-Apr-12
ManningB 00419503	ManningB 00419503	12-Apr-12
ManningB 00419504	ManningB 00419516	12-Apr-12
ManningB 00419517	ManningB 00419517	12-Apr-12
ManningB 00419518	ManningB 00419518	12-Apr-12
ManningB 00419521	ManningB 00419521	12-Apr-12
ManningB 00419574	ManningB 00419596	12-Apr-12
ManningB 00419627	ManningB 00419638	12-Apr-12
ManningB 00419657	ManningB 00419657	12-Apr-12

From: David Coombs [coombs@armycourtmarshaldefense.com]
Sent: Wednesday, April 25, 2012 9:38 PM
To: denise.lind@us.army.mil
Cc: Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; joshua.j.tooman.mil@mail.mil; Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA; melissa.s.santiago.mil@mail.mil; VonElten, Alexander S. 1LT USA JFHQ-NCR/MDW SJA; Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA
Subject: RE: 380-5

Ma'am,

Pursuant to your questions earlier today, the Defense wanted to follow-up on two points:

1) Whether AR 380-5 is Punitive

As the Defense argued, AR 380-5 is a punitive regulation. If you look at the section we have been talking about, it is entitled "Corrective Measures and Sanctions." I reproduced the relevant sections below for your review:

Section VII

Corrective Actions and Sanctions

1-20. General

Commanders will establish procedures to make sure that prompt and appropriate action is taken concerning a violation of the provisions of this regulation, especially in those cases involving incidents which can put classified information at risk of compromise, unauthorized disclosure, or improper classification of information. Such actions will focus on a correction or elimination of the conditions that caused or contributed to the incident.

1-21. Sanctions

a. DA personnel will be subject to sanctions if they knowingly, willfully, or negligently—

- (1) Disclose classified or sensitive information to unauthorized persons.
- (2) Classify or continue the classification of information in violation of this regulation.
- (3) Violate any other provision of this regulation.

b. Sanctions can include, but are not limited to warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and removal of original classification authority. Action can also be taken under the Uniform Code of Military Justice (UCMJ) for violations of that Code and under applicable criminal law, if warranted.

c. Original classification authority will be withdrawn for individuals who demonstrate a disregard or pattern of error in applying the classification and sensitivity standards of this regulation.

There is no clearer evidence that this section was entitled to be punitive than the fact that the word “sanctions” is used four times and the word “violation” (or a variation thereof) is used three times.

2) Whether there is a Distinction Between “Intelligence Information” and “Classified and Sensitive” Information

The Government argued that there is a distinction between “intelligence” (as charged under Article 134) on the one hand, and “classified” and “sensitive” information, on the other. In their motion, they argue that “intelligence is not limited only to classified or sensitive information.” (p. 7). The Government does not provide any authority to support the view that “intelligence” is not limited to classified or sensitive information (or, otherwise stated, that “intelligence” is broader than classified or sensitive information). They simply point to the Article 104 instruction in the Benchbook, which states that “intelligence” must be true, at least in part. The section does not comprehensively define intelligence. The Government is proceeding from the understanding that “intelligence” is broader than just classified or sensitive information. The Defense does not believe this is true – it submits that “intelligence” is coextensive with classified or sensitive information (at least as charged in this case).

Moreover, the Defense would note that the Government's definition of "sensitive" information is derived from section 5-19 of AR 380-5, which defines sensitive information for the purpose of the Computer Security Act of 1987, not for the purpose of AR 380-5. "Sensitive" information for the purpose of the Regulation is not defined. Thus it appears that when AR 380-5 is using "sensitive" in section 1-21 it is not using this word as a term of art or defined term.

As stated, the Defense believes that "intelligence" (as charged in Article 134) is the same as "classified" and "sensitive" information in AR 380-5. In this respect, the Defense would note the following:

a. AR 380-5: The Regulation's purpose is as follows:

1-1. Purpose

This regulation establishes the policy for the classification, downgrading, declassification, transmission, transportation, and safeguarding of information requiring protection in the interests of national security.

The Regulation is 311 pages long. It covers every conceivable aspect of information assurance. It is difficult to believe that the Army would only intend for this Regulation to cover "classified" and "sensitive" information (and to punish disclosures of such information), but that there would be other "intelligence" out there that the Regulation did not intend to reach. In other words, the Government believes that there is information that does not qualify as "classified" or "sensitive" but that is nonetheless "intelligence." To accept this argument is to accept that the Army has left completely unregulated a whole area of "intelligence" to simply be dealt with otherwise than by regulation.

b. Video Alleged in Specification 2: The Government points to a charged video as being an example of something that falls within "intelligence" but does not fall under "classified" or "sensitive" information within the meaning of AR 380-5. The Defense believes that the video squarely falls within the definition of sensitive information as intended in AR 380-5. Even if we were to accept the definition of sensitive offered by the government ("Any information, the loss,

misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, USC (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.”), it is clear that the video, as charged, meets the definition of sensitive. The Government has charged PFC Manning with transmitting “information relating to the national defense [the video] ... with reason to believe such information could be used to the injury of the United States or to the advantage of any foreign nation.” Thus, the Government believes that the video could be used to the injury of the United States or to the advantage of a foreign nation. It would seem to follow then that the improper release of the video “could adversely affect the national interest” (i.e. the Government’s definition of sensitive). There is no information charged that is not classified or sensitive within the meaning of AR 380-5.

c. AR 380-5’s Use of “Intelligence Information” – AR 380-5 seems to suggest that “intelligence” is actually synonymous with a subset of classified information. For instance, section D-1 reads:

Security Controls on Dissemination and Marking of Warning Notices on Intelligence Information

D-1. General

Intelligence information will be controlled and marked in accordance with Director of Central Intelligence Directive (DCID) 1/7, “Security Controls on the Dissemination of Intelligence Information”, included as figure D-1 of this appendix, and future revisions. Control markings as well as all other policy stipulated in DCID 1/7 apply solely to intelligence information and not to other classified information. Except as specifically stipulated in this appendix, intelligence information will be safeguarded in the same manner as other types of classified information of the same classification level.

This section seems to support the view that “intelligence” (or more specifically “intelligence information”) is actually a sub-set of classified information. In other words, it is narrower than classified information, not broader.

In short, the Defense does not believe that “intelligence” is broader than either classified or sensitive information within the meaning of AR 380-5. It was clear what the Army intended to accomplish in enacting AR 380-5: it intended to punish unauthorized disclosures of protected information (whether we call that information “classified”/“sensitive” or “intelligence”).

Accordingly, the Defense submits that because there is a punitive regulation which squarely addresses all the charged documents, the offense must be charged as an Article 92 offense and not a 134 offense.

The Government believes that because AR 380-5 does not deal with the specific manner in which information is disclosed (i.e. through the internet), then the regulation is not applicable. This is not the case. AR 380-5, section 1-21a.(1) states that "DA personnel will be subject to sanctions if they knowingly, willfully, or negligently - (1) disclose classified or sensitive information to unauthorized persons." It does not matter how this unauthorized disclosure is carried out (through the internet, over the phone, in person, by email, etc.). What matters is that there is a lawful general regulation that prohibits disclosure of information, however that disclosure is done.

Finally, the Government's email confuses preemption (the Defense's first argument) with the rule in Borunda (the Defense's second argument). The issue of AR 380-5 deals with the latter issue (i.e. the rule in Borunda) and not preemption. Accordingly, the Government's purported distinguishing of McGuinness is inapposite, as that case deals with preemption.

v/r

David

David E. Coombs, Esq.

Law Office of David E. Coombs

11 South Angell Street, #317

Providence, RI 02906

Toll Free: 1-800-588-4156

Local: (508) 689-4616

Fax: (508) 689-9282

coombs@armycourtartialdefense.com

www.armycourtartialdefense.com

Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.

-----Original Message-----

From: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA [mailto:Ashden.Fein@jfhqncr.northcom.mil]

Sent: Wednesday, April 25, 2012 7:27 PM

To: denise.lind@us.army.mil

Cc: coombs@armycourtartialdefense.com; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; joshua.j.tooman.mil@mail.mil; Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA; melissa.s.santiago.mil@mail.mil; VonElten, Alexander S. 1LT USA JFHQ-NCR/MDW SJA
Subject: 380-5

Ma'am. Ultimately, the United States agrees that AR 380-5 is punitive in nature; however just because a regulation is punitive in nature, not all provisions within the regulation are punitive. For example, AR 25-2 sets forth "bolded" paragraphs which highlight the exact provisions which are punitive. There are portions of AR 380-5 that are punitive in nature, but those provisions follow after Chapter 1, with the specified prohibited conduct, such as storing classified information at a residence (paragraph 7-6), knowingly or willfully disclosing classified information (paragraph

10-11 through -23), or negligently violating the regulation (paragraph 10-10). Specifically, Chapter 1 of AR 380-5 is titled "General Provisions and Program Management." Other provisions within Chapter 1 of AR 380-5 include an explanation of abbreviations and terms (1-3), the responsibilities of the Secretary of the Army (1-4), the scope of the regulation (1-10), background information (1-

14). Most regulations, like AR 380-5, contain background information on the regulation upfront, to include AR 380-5, para.

1-21. Paragraph 1-21, Subsection (b) thereof sets out the sanctions available for disclosing such information, to include, without limitation, warning, reprimand, action under UCMJ, and action under applicable criminal law. See AR 380-5, para. 1-21b. The United States does not dispute that other provisions contained within AR 380-5 are punitive. See AR 380-5, para.

10-10 (subjecting persons to administrative sanctions if they negligently disclose, to unauthorized persons).

However, if the Court finds Paragraph 1-21 is punitive, then Specification 1 of Charge II is not preempted by Article 92. In addition to what has already been provided in the government's written response and argument today, Paragraph 1-21 does not hold a Soldier criminally responsible for wrongful and wantonly causing intelligence to be published on the internet, but only the knowing, willful, or negligent disclosure of classified or sensitive information to unauthorized persons. In McGuinness, the Court of Military Appeals actually held that the Navy regulation (comparable to AR 380-5) which prohibited storing classified information at an individual's residence was not preempted by a violation of 18 USC 793 for the same type of offense. The Court stated that nothing in the legislative history of Article 92 provided that Congress intended general orders / regulations to occupy the field for offenses that could be charged under Article 134. Although the McGuinness Court applied this standard to a Clause 3 offense (18 USC 793(e)), the United States cannot find any contrary case law which would not apply this to a Clause 1 and 2 offense. Finally, there is no evidence that the Army intended AR 380-5 to cover the field for causing intelligence to be published on the internet or even disclosure of classified, or sensitive information or intelligence to unauthorized individuals, evidenced by multiple other punitive laws/regulations that touch on this subject, such as AR 530-1 (paragraph 2-1), Articles 104, 106a.

In McGuinness, the Court found that paragraph 7-6, AR 380-5 was punitive.

Paragraph 7-4 if found within the same section as paragraph 7-6 and contains similar prohibiting language about storing classified information.

Vr Maj Fein

Williams, Patricia CIV JFHQ-NCR/MDW SJA

From: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA
Sent: Wednesday, April 25, 2012 7:27 PM
To: 'denise.lind@us.army.mil'
Cc: 'combs@armycourt.martialdefense.com'; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; 'joshua.j.tooman.mil@mail.mil'; Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA; 'melissa.s.santiago.mil@mail.mil'; VonElten, Alexander S. 1LT USA JFHQ-NCR/MDW SJA
Subject: 380-5

Ma'am. Ultimately, the United States agrees that AR 380-5 is punitive in nature; however just because a regulation is punitive in nature, not all provisions within the regulation are punitive. For example, AR 25-2 sets forth "bolded" paragraphs which highlight the exact provisions which are punitive. There are portions of AR 380-5 that are punitive in nature, but those provisions follow after Chapter 1, with the specified prohibited conduct, such as storing classified information at a residence (paragraph 7-6), knowingly or willfully disclosing classified information (paragraph 10-11 through -23), or negligently violating the regulation (paragraph 10-10). Specifically, Chapter 1 of AR 380-5 is titled "General Provisions and Program Management." Other provisions within Chapter 1 of AR 380-5 include an explanation of abbreviations and terms (1-3), the responsibilities of the Secretary of the Army (1-4), the scope of the regulation (1-10), background information (1-14). Most regulations, like AR 380-5, contain background information on the regulation upfront, to include AR 380-5, para. 1-21. Paragraph 1-21, Subsection (b) thereof sets out the sanctions available for disclosing such information, to include, without limitation, warning, reprimand, action under UCMJ, and action under applicable criminal law. See AR 380-5, para. 1-21b. The United States does not dispute that other provisions contained within AR 380-5 are punitive. See AR 380-5, para. 10-10 (subjecting persons to administrative sanctions if they negligently disclose, to unauthorized persons).

However, if the Court finds Paragraph 1-21 is punitive, then Specification 1 of Charge II is not preempted by Article 92. In addition to what has already been provided in the government's written response and argument today, Paragraph 1-21 does not hold a Soldier criminally responsible for wrongful and wantonly causing intelligence to be published on the internet, but only the knowing, willful, or negligent disclosure of classified or sensitive information to unauthorized persons. In McGuinness, the Court of Military Appeals actually held that the Navy regulation (comparable to AR 380-5) which prohibited storing classified information at an individual's residence was not preempted by a violation of 18 USC 793 for the same type of offense. The Court stated that nothing in the legislative history of Article 92 provided that Congress intended general orders / regulations to occupy the field for offenses that could be charged under Article 134. Although the McGuinness Court applied this standard to a Clause 3 offense (18 USC 793(e)), the United States cannot find any contrary case law which would not apply this to a Clause 1 and 2 offense. Finally, there is no evidence that the Army intended AR 380-5 to cover the field for causing intelligence to be published on the internet or even disclosure of classified, or sensitive information or intelligence to unauthorized individuals, evidenced by

multiple other punitive laws/regulations that touch on this subject, such as AR 530-1 (paragraph 2-1), Articles 104, 106a.

In McGuiness, the Court found that paragraph 7-6, AR 380-5 was punitive. Paragraph 7-4 if found within the same section as paragraph 7-6 and contains similar prohibiting language about storing classified information.

Vr Maj Fein



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
U.S. ARMY MILITARY DISTRICT OF WASHINGTON
103 THIRD AVENUE
FORT LESLEY J. MCNAIR, DC 20319-5013

ANCG

4 MAY 2012

MEMORANDUM FOR PFC Bradley E. Manning, Headquarters and Headquarters Company,
U.S. Army Garrison, Joint Base Myer-Henderson Hall, Fort Myer, VA 22211

SUBJECT: Request for Individual Military Counsel (IMC) – PFC Bradley E. Manning

I have reviewed your request for Individual Military Counsel (IMC) and the Memorandum from COL Mark Cremin, Chief, U.S. Army Trial Defense Service, Fort Belvoir, VA. COL Cremin determined that there is an attorney-client relationship and MAJ Thomas F. Hurley is reasonably available to act as your Individual Military Counsel (IMC). Your request is approved IAW AR 27-10, paragraph 5-7 and 6-10.

2 Encls

1. Chief, USATDS Memo, 1 May 12
2. IMC Request, 25 Apr 12

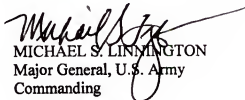

MICHAEL S. LINNINGTON
Major General, U.S. Army
Commanding

TABLE OF CONTENTS

- TAB 1 - ERB
- TAB 2 - Chief, USATDS Memo, 1 May 12
- TAB 3 - Request for IMC, U.S. v. Manning, 27 Apr 12
- TAB 4 - Charge Sheet, U.S. v. Manning



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
U.S. ARMY TRIAL DEFENSE SERVICE
Office of the Chief
9276 Gunston Road
Fort Belvoir, VA 22060

JALS-TD

1 May 2012

MEMORANDUM THRU PFC Bradley E. Manning

FOR OFFICE OF THE STAFF JUDGE ADVOCATE, Military District of Washington

SUBJECT: Request for Individual Military Counsel (IMC) – MAJ Thomas F. Hurley

1. I have carefully considered PFC Bradley E. Manning's request for individual military counsel (IMC) under the provisions of Rule for Courts-Martial 506(b) and paragraphs 5-7 and 6-10, Army Regulation (AR) 27-10, *Military Justice*. I have determined that the requested counsel, MAJ Thomas F. Hurley, is reasonably available and that there is a prior attorney-client relationship that lasted for several weeks in 2010.
2. As described in AR 27-10, para. 5-7 (f)(1)(a), the approval authority for this request is the convening authority. In my capacity as the Chief, Trial Defense Service, I strongly recommend that the subject request be granted.
3. POC for this action is my Executive Officer, LTC Elizabeth Sweetland at elizabeth.sweetland.mil@mail.mil or (703) 693-0283.

for Elizabeth Sweetland LTC, JA
MARK CREMIN
COL, JA
Chief, US Army Trial Defense Service

25 April 2012

MEMORANDUM FOR RECORD

SUBJECT: Request for Individual Military Counsel in U.S. v. PFC Bradley E. Manning

1. References.

a. Manual for Courts-Martial (MCM), 2010

b. Army Regulation (AR) 27-10, "Military Justice," dated 16 November 2005.

2. Pursuant to sections 5-7 and 6-10 of AR 27-10 and Rule for Courts-Martial (R.C.M.) 506(b), I hereby request that Major (MAJ) Thomas Hurley be detailed as Individual Military Counsel (IMC) to my case, U.S. v. Private First Class (PFC) Bradley E. Manning. I request MAJ Hurley as an addition to my current detailed military counsel, Captain (CPT) Joshua Tooman.

3. Background.

a. In summer 2010, I was detailed CPT Paul Bouchard as military counsel. Immediately following transfer to the Pretrial Confinement Facility (PCF) at Marine Corps Base (MCB) Quantico, Virginia, MAJ Hurley was assigned to the defense team in order to ease the transition from theater to the continental United States until assigned permanent defense counsel. After being detailed MAJ Matthew Kemkes as additional counsel in August 2010, MAJ Hurley was removed from the defense team. I also requested IMC for CPT Bouchard to stay on the case.

b. On 01 September 2010, I hired Mr. David Coombs as my civilian defense counsel. I elected to keep my detailed military counsel, MAJ Kemkes and CPT Bouchard, in order to assist Mr. Coombs. After transferring to the Joint Regional Correctional Facility (JRCF) at Fort Leavenworth, Kansas in April 2011, CPT Joshua Tooman was assigned as an assistant to the case.

c. Most recently, on 13 April 2012, I elected to excuse both of my detailed military defense counsel, MAJ Kemkes and CPT Bouchard, and requested that CPT Tooman be detailed as full-time military defense counsel.

SUBJECT: Request for Individual Military Counsel in U.S. v. PFC Bradley E. Manning

4. Presently, my defense team consists of one civilian defense counsel, one military defense counsel, and one legal administrator, namely:

- a. Mr. David Coombs, Civilian Defense Counsel.
- b. CPT Joshua Tooman, Defense Counsel.
- c. WO1 Melissa Santiago, Legal Administrator.

5. In contrast, the prosecution presently consists of at least four officers as trial counsel and one legal administrator out of the Military District of Washington (MDW) Office of the Staff Judge Advocate (OSJA), namely:

- a. MAJ Ashden Feyn, Trial Counsel.
- b. CPT JoDean Morrow III, Assistant Trial Counsel.
- c. CPT Angel Overgaard, Assistant Trial Counsel.
- d. CPT Jeffrey Whyte, Assistant Trial Counsel.
- e. WO1 Arthur Ford, Legal Administrator.

6. Currently, there is an uneven representation, of at least two full-time military counsel, between myself and my defense team, and the government and prosecution team. I therefore make this request primarily to compensate for the difference between the defense and prosecution. Otherwise Mr. Coombs, my civilian defense counsel will take on an unfair burden of the work load in my case. As noted above, the teams were much closer to even when I had two part-time detailed military counsel to assist Mr. Coombs.

7. I am providing the following information, required under paragraph 5-7(f)(2) of AR 27-10, to process this IMC request.

a. Name, grade and station of requested counsel. MAJ Thomas Hurley, U.S. Army Trial Defense Service (USATDS), DCAP, Arlington, Virginia 22203.

b. Name, grade and station of accused and existing defense counsel.

(1) PFC Manning, Headquarters and Headquarters Company (HHC), U.S. Army Garrison (USAG), Joint Base Myer-Henderson Hall, Fort Myer, Virginia 22211.

(2) CPT Joshua Tooman, USATDS, Fort Leavenworth, Kansas 66027.

SUBJECT: Request for Individual Military Counsel in U.S. v. PFC Bradley E. Manning

c. Charges and summary of charges.

(1) Five (5) specifications of violating a lawful general regulation under Article 92, UCMJ (Section 892, Title 10 U.S.C.)

(2) One (1) specification of aiding the enemy under Article 104, UCMJ (Section 904, Title 10 U.S.C.)

(3) One (1) specification of disorders and neglects to the prejudice of good order and discipline and service discrediting, eight (8) specifications of communicating classified information (Section 793(e), Title 18 U.S.C.), five (5) specifications of stealing or knowingly converting government property (Section 641, Title 18 U.S.C.), and two (2) specifications of knowingly exceeding authorized access to a government computer (Section 1030(a)(1), Title 18 U.S.C.) under Article 134, UCMJ (Section 934, Title 10 U.S.C.)

d. Date charges preferred and status of case. The original charges were preferred on 05 July 2010. Those charges were dismissed by the convening authority on 18 March 2011. The current charges were preferred on 01 March 2011. On 16 December through 22 December 2011, those charges were investigated by an Investigating Officer (IO) pursuant to Article 32(b), UCMJ (Section 832(b), Title 10, U.S.C.) The charges were referred, without special instructions, to a general court-martial on 03 February 2012.

e. Date and form of pretrial restraint. Ordered into pretrial confinement on 29 May 2010. In confinement at Camp Arifjan, Kuwait until transferred to Quantico, Virginia on 29 July 2010. Later transferred to Fort Leavenworth, Kansas on 20 April 2011. Periodic transfers near Fort Meade for pretrial hearings.

f. Anticipated date and length of trial. Presently expected to be twenty-one (21) days between September and December 2012 at Fort Meade, Maryland.

g. Existence of attorney-client relationship. As mentioned above, MAJ Hurley was previously assigned in August 2010 as an assistant to my case until MAJ Kemkes was permanently detailed as military counsel.

h. Special circumstances or other factors relating to availability. MAJ Hurley's current duty station is within the MDW, near the same location as the prosecution, Fort McNair, D.C., and the pretrial hearings and trial, Fort Meade, Maryland.

SUBJECT: Request for Individual Military Counsel in U.S. v. PFC Bradley E. Manning

8. I understand the decision to request for and retain military defense counsel is my own decision. No one has forced or coerced me into making this request. I appreciate the charges in this case. I understand the maximum punishment for the offenses is a dishonorable discharge, reduction to lowest enlisted pay grade (E-1), total forfeitures of pay and allowances, and confinement for life without the possibility of parole.

9. The point of contact (POC) for this memorandum is the undersigned at HHC, USAG, 239 Sheridan Avenue, Building 417, Joint Base Myer-Henderson Hall, Fort Myer, Virginia 22211.

A handwritten signature in dark ink, appearing to read 'B. Manning', is written over the typed name.

BRADLEY E. MANNING
PFC, U.S. Army

27 April 2012

MEMORANDUM FOR RECORD

SUBJECT: Addendum to Request for Individual Military Counsel in U.S. v. PFC Bradley E. Manning

1. I have recently been informed that the Government added an additional trial counsel to their team. The Government now has 1LT Alexander S. VonElten on its team. The added counsel provides additional support for my Individual Military Counsel request.
2. The Point of Contact (POC) for this memorandum is the undersigned at HHC, USAG, 239 Sheridan Avenue, Building 417, Joint Base Myer-Henderson Hall, Fort Myer, Virginia 22211.



BRADLEY MANNING
PFC, U.S. Army

ORB TYPE 2900	BRIEF DATE 20120603	JUNCTIONAL CATEGORY JAG BRANCH	DESIG DATE	CNTL BRANCH JA	COMPONENT RA	AD GRADE-ADDER MAJ	SSN 20060410 444-86-6197	NAME HURLEY THOMAS FREDRICK	
SECTION I - Assignment Information				SECTION II - Security Data		SECTION III - Service Data		SECTION IV - Personal/Family Data	
OVERSEAS DEPLOYMENT / COMBAT DUTY				INVEST SSB		BASD 19961020 Current PPN D5		Date of Birth 19710608 Birthplace OKLAHOMA	
End Date	CT	MO	Y	T	NUMBER OF TOURS	DTENR 20071205 DTPSCG 20080319	Basic Date of Apt 19930529 Cohort Yr Gp FY1997	Country of Cit US Sex/Rescat M /WHITE NOT HISP	
20081224	12	14	1	C	Short- 1 Long- 0	CLNC YS-SCI	Mo/Days Altia 191/11 Mo/Als 191	No of Dependent Adults/Children 0100 Religion PROT-OTHER	
DROS NA DEROS NA #MILPO Tour Data CBT- 1 OPN- 0 RES- 0 Dwell Start 20081224 Dwell Mo-Days 40Mo 28D				SECTION V - Foreign Language		Language L S R YMPTL 2LT-W01 1LT-CW2 CPT-CW3 MAJ-CW4 PDOR 19970207 19990301 20060410 TDOR LTG GEN		Date of Dependent Adults/Children 0100 Spouse Birthplace/Cit OKLAHOMA/US Mental Status MARRIED Pulses/Date 111111/20110510 Height/Weight 72/226	
Date Dependents Arrived OS				DLAT		PDOR 19970207 19990301 20060410 TDOR LTG GEN		Home of Record at End OKLAHOMA Mailing Address	
Career Field Information - Commissioned/AMEDD/Warrant				SECTION VI - Military Education		SECTION VII - Civilian Education		SECTION X - Remarks	
BR Code/Med/Mos/1Pmos				CSC GRAD		LEVEL COMPLETED		6156 CORBS RD ALEXANDRIA VA 22310-0000 DATE LAST PHOTO TAKEN NAME, AGE, SEX, COMB	
Functl Area/Med/Mos/2/Smos				Course		INSTITUTION VA THE JAG SCHOOL LLM K YR 2006 DISCIPLINE MILITARY LAW INSTITUTION OK U OK NORMAN CAMPUS JD G YR 1996 DISCIPLINE LAW, GENERAL INSTITUTION OK EAST CENTRAL U. ADA BA G YR 1993 DISCIPLINE ENGLISH			
BRAOC/Med/Mos/3Pmos Sg A				Year		SECTION VIII - Awards and Decorations			
Skills 3P 5P				ILE QUALIFICATION 2009 ILE COMMON CORE 2009 JA OFF GRAD CRSE 2006 CAS3 2003 JUDGE ADVOC OFF BASIC 1998 FA BOLD 1997 AIRBORNE 1991		BSM- 1 ASR- 1 MSM- 2 OSR- 1 ARCOM- 4 PRICHTBAD- 1 AAM- 1 NDSM- 2 ICMS- 1 GWOTS- 1			
Basic Branch/FMOS JAG CORPS				ILE QUALIFICATION 2009 ILE COMMON CORE 2009 JA OFF GRAD CRSE 2006 CAS3 2003 JUDGE ADVOC OFF BASIC 1998 FA BOLD 1997 AIRBORNE 1991		BSM- 1 ASR- 1 MSM- 2 OSR- 1 ARCOM- 4 PRICHTBAD- 1 AAM- 1 NDSM- 2 ICMS- 1 GWOTS- 1			
Functional Area SMOCS				ILE QUALIFICATION 2009 ILE COMMON CORE 2009 JA OFF GRAD CRSE 2006 CAS3 2003 JUDGE ADVOC OFF BASIC 1998 FA BOLD 1997 AIRBORNE 1991		BSM- 1 ASR- 1 MSM- 2 OSR- 1 ARCOM- 4 PRICHTBAD- 1 AAM- 1 NDSM- 2 ICMS- 1 GWOTS- 1		DATE LAST PHOTO TAKEN NAME, AGE, SEX, COMB	
Career Track X Single Dual				ILE QUALIFICATION 2009 ILE COMMON CORE 2009 JA OFF GRAD CRSE 2006 CAS3 2003 JUDGE ADVOC OFF BASIC 1998 FA BOLD 1997 AIRBORNE 1991		BSM- 1 ASR- 1 MSM- 2 OSR- 1 ARCOM- 4 PRICHTBAD- 1 AAM- 1 NDSM- 2 ICMS- 1 GWOTS- 1			
Privacy X Branch Functional Area				ILE QUALIFICATION 2009 ILE COMMON CORE 2009 JA OFF GRAD CRSE 2006 CAS3 2003 JUDGE ADVOC OFF BASIC 1998 FA BOLD 1997 AIRBORNE 1991		BSM- 1 ASR- 1 MSM- 2 OSR- 1 ARCOM- 4 PRICHTBAD- 1 AAM- 1 NDSM- 2 ICMS- 1 GWOTS- 1			
Prev Branch/MOS 13				ILE QUALIFICATION 2009 ILE COMMON CORE 2009 JA OFF GRAD CRSE 2006 CAS3 2003 JUDGE ADVOC OFF BASIC 1998 FA BOLD 1997 AIRBORNE 1991		BSM- 1 ASR- 1 MSM- 2 OSR- 1 ARCOM- 4 PRICHTBAD- 1 AAM- 1 NDSM- 2 ICMS- 1 GWOTS- 1			
Prev Functional Area				ILE QUALIFICATION 2009 ILE COMMON CORE 2009 JA OFF GRAD CRSE 2006 CAS3 2003 JUDGE ADVOC OFF BASIC 1998 FA BOLD 1997 AIRBORNE 1991		BSM- 1 ASR- 1 MSM- 2 OSR- 1 ARCOM- 4 PRICHTBAD- 1 AAM- 1 NDSM- 2 ICMS- 1 GWOTS- 1			
Control Career Management Field 27A00				ILE QUALIFICATION 2009 ILE COMMON CORE 2009 JA OFF GRAD CRSE 2006 CAS3 2003 JUDGE ADVOC OFF BASIC 1998 FA BOLD 1997 AIRBORNE 1991		BSM- 1 ASR- 1 MSM- 2 OSR- 1 ARCOM- 4 PRICHTBAD- 1 AAM- 1 NDSM- 2 ICMS- 1 GWOTS- 1		DATE LAST PHOTO TAKEN NAME, AGE, SEX, COMB	
Projected Career Management Field 27A00				ILE QUALIFICATION 2009 ILE COMMON CORE 2009 JA OFF GRAD CRSE 2006 CAS3 2003 JUDGE ADVOC OFF BASIC 1998 FA BOLD 1997 AIRBORNE 1991		BSM- 1 ASR- 1 MSM- 2 OSR- 1 ARCOM- 4 PRICHTBAD- 1 AAM- 1 NDSM- 2 ICMS- 1 GWOTS- 1			
Geographic Orientation				ILE QUALIFICATION 2009 ILE COMMON CORE 2009 JA OFF GRAD CRSE 2006 CAS3 2003 JUDGE ADVOC OFF BASIC 1998 FA BOLD 1997 AIRBORNE 1991		BSM- 1 ASR- 1 MSM- 2 OSR- 1 ARCOM- 4 PRICHTBAD- 1 AAM- 1 NDSM- 2 ICMS- 1 GWOTS- 1			
ASST AVIATOR QUALIFICATIONS				ILE QUALIFICATION 2009 ILE COMMON CORE 2009 JA OFF GRAD CRSE 2006 CAS3 2003 JUDGE ADVOC OFF BASIC 1998 FA BOLD 1997 AIRBORNE 1991		BSM- 1 ASR- 1 MSM- 2 OSR- 1 ARCOM- 4 PRICHTBAD- 1 AAM- 1 NDSM- 2 ICMS- 1 GWOTS- 1			
Pilot Status				ILE QUALIFICATION 2009 ILE COMMON CORE 2009 JA OFF GRAD CRSE 2006 CAS3 2003 JUDGE ADVOC OFF BASIC 1998 FA BOLD 1997 AIRBORNE 1991		BSM- 1 ASR- 1 MSM- 2 OSR- 1 ARCOM- 4 PRICHTBAD- 1 AAM- 1 NDSM- 2 ICMS- 1 GWOTS- 1			
Raising Date				ILE QUALIFICATION 2009 ILE COMMON CORE 2009 JA OFF GRAD CRSE 2006 CAS3 2003 JUDGE ADVOC OFF BASIC 1998 FA BOLD 1997 AIRBORNE 1991		BSM- 1 ASR- 1 MSM- 2 OSR- 1 ARCOM- 4 PRICHTBAD- 1 AAM- 1 NDSM- 2 ICMS- 1 GWOTS- 1		DATE LAST PHOTO TAKEN NAME, AGE, SEX, COMB	
Date of Last PCS 20090417				ILE QUALIFICATION 2009 ILE COMMON CORE 2009 JA OFF GRAD CRSE 2006 CAS3 2003 JUDGE ADVOC OFF BASIC 1998 FA BOLD 1997 AIRBORNE 1991		BSM- 1 ASR- 1 MSM- 2 OSR- 1 ARCOM- 4 PRICHTBAD- 1 AAM- 1 NDSM- 2 ICMS- 1 GWOTS- 1			
SECTION IX-Assignment Information				Date of Last DER 20110528		Org Zip Code 22060			
ASGT	FROM	MO	UNIT NO	ORGANIZATION	STATION	LOC	COMD		DUTY TITLE
PROJ	20120715		W46F	USA ELE DF LEGAL SVC	PENTAGON	7 VA	DF		REG NR OTJ
Current	20100528		W0KE	USA LEGAL SERVICES A	FT BELVOIR	7 VA	FA	DEPUTY DCA	
1st Prev	20090428	13	W0KE	USA LEGAL SERVICES A	ARLINGTON	7 VA	FA	CSIS FELLOW	
2nd Prev	20081224	04	0003	AR HHC D4 BDE	FT STEWAR	1 GA	FC	BRIGADE JUDGE ADVOCATE	
3rd Prev	20071027	14	0003	AR HHC D4 BDE	FOB KALSU	1 IZ	CC	BRIGADE JUDGE ADVOCATE	
4th Prev	20060630	16	0003	AR HHC D4 BDE	FT STEWAR	1 GA	FC	BRIGADE JUDGE ADVOCATE	
5th Prev	20040621	13	W0KE	USA TRIAL DEFENSE SVC	FT SILL	5 OK	SE	SENIOR DEFENSE COUNSEL	
6th Prev	20020701	23	W0KE	USA TRIAL DEFENSE SVC	FT MYER	1 VA	FC	TRIAL DEFENSE COUNSEL	
7th Prev	20001015	20	0019	AG DET STRAF REPL	FT BRAGG	1 NC	FC	TRIAL COUNSEL	
8th Prev	19990712	03	0018	HO HHC ABN CORPS	FT BRAGG	1 NC	FC	OPERATIONAL LAW ATTORNEY	
9th Prev	19981026	14	0018	HO HHC ABN CORPS	FT BRAGG	1 NC	FC	LEGAL ASSISTANCE ATTY	
10th Prev	19980416	06	W0VQ	H4HB P S BN USAFACPS	FT SILL	5 OK	TC	SPEC ASST TRIAL COUNSEL	
11th Prev	19971104	06	0032	FA BN 06MLRS C BTRY	FT SILL	5 OK	FC	PLATOON LEADER	
12th Prev	19970412	07	0032	FA BN 06MLRS HHS	FT SILL	5 OK	FC	PLATOON LEADER	
13th Prev									
14th Prev									
15th Prev									
16th Prev									
17th Prev									
18th Prev									
19th Prev									

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)
U.S. Army, xxx-xx-)
Headquarters and Headquarters Company,)
U.S. Army Garrison, Joint Base Myer-)
Henderson Hall, Fort Myer, VA 22211)

**RULING: Government
Motion to Reconsider Ruling:
Department of State Damage
(DOS) Assessment**

DATED: 11 May 2012

The Government moves the Court to reconsider its 23 March 2012 ruling requiring the Government by 18 May 2012 to:

1. disclose to the Defense, any unclassified information from the DOS damage assessment that is favorable to the accused and material to guilt or punishment;
2. disclose to the Court, any additional unclassified information from the DOS damage assessment not disclosed to the defense for *in camera review*.
3. identify what classified information in the DOS damage assessment is favorable to the defense and material to guilt or punishment; and
4. disclose to the Court all classified information in the DOS damage assessment for *in camera review* IAW RCM 701(g)(2) or, at the request of the Government, *in camera review* for limited disclosure under MRE 505(g)(2).

The Government moves the Court to rule that the State Department Damage Assessment is a draft, and, therefore, any information contained in it is not discoverable because of its speculative nature. The Defense opposes.

The Government has provided the Court and Defense Counsel with a classified letter from DOS with background information explaining the draft nature of the DOS Damage Assessment. The Government has also provided the Court with the classified DOS Damage Assessment for *in camera review* to rule on this motion.

The Court has examined both the classified letter and the classified DOS Damage Assessment and finds that the DOS Damage Assessment is a draft damage assessment. The fact that it is a draft does not make the draft speculative or not discoverable under RCM 701.

RULING: The Government Motion to Reconsider the Court's ruling of 23 March 2012 with respect to the DOS Damage Assessment is **GRANTED**. Having reconsidered the 23 March 2012 ruling, the Government Motion to Find the DOS Draft Damage Assessment not discoverable is **DENIED**. The Government will comply with the 23 March 2012 ruling of the Court.

So Ordered this 11th day of May 2012.



DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

**Prosecution Notification
to the Court**

2 May 2012

The United States supplements its 20 April 2012 response to the Court's Order, dated 23 March 2012, as follows:

1. The prosecution contacted the CIA to determine whether this agency contains any forensic results or investigative files relevant to this case.¹

CIA. The CIA has investigative files. The United States reviewed this information for evidence that is favorable to the accused and material to either guilt or punishment.

2. At this time, the United States anticipates that the **FBI** and **CIA** are the only government entities that are custodians of classified forensic results or investigative files relevant to this case that will seek limited disclosure IAW MRE 505(g)(2).



ASHDEN FEIN
MAJ, JA
Trial Counsel

¹ On 16 April 2012, the Court granted the Government's motion for leave of the Court to extend the time to respond from 20 April 2012 to 2 May 2012 as to whether the CIA will release classified information in original form, provide for limited disclosure under MRE 505(g)(2), or invoke the classified information privilege under MRE 505(c). This filing is in response to this extension of time.

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army, xxx-xx-)

Headquarters and Headquarters Company, U.S.)

Army Garrison, Joint Base Myer-Henderson Hall,)

Fort Myer, VA 22211)

**DEFENSE MOTION TO DISMISS
SPECIFICATIONS 2, 3, 5, 7, 9, 10,
11 AND 15 OF CHARGE II**

DATED: 10 May 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, pursuant to applicable case law, Rule for Courts Martial (R.C.M.) 907(a), R.C.M. 907(b)(1)(B), and the First and the Fifth Amendments to the United States Constitution, requests this Court to dismiss Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II because 18 U.S.C. Section 793(e) is unconstitutionally vague in violation of the Fifth Amendment and substantially overbroad in violation of the First Amendment. In the alternative, the Defense requests this Court to provide limiting instructions that narrow the breadth of Section 793(e) and more clearly define its vague terms.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. The Defense, as the moving party, bears the burden of this motion by a preponderance of the evidence pursuant to R.C.M. 905(c)(1) and (2)(A).

FACTS

3. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of conduct prejudicial to good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting government property, and two specifications of knowingly exceeding authorized access to a government computer, in violation of Articles 92, 104, and 134, UCMJ, 10 U.S.C. §§ 892, 904, 934 (2010). Specifically, in Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II, PFC Manning is charged with unauthorized possession and disclosure of classified information in violation of Section 793(e). See Charge Sheet.

WITNESSES/EVIDENCE

4. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this Court to consider the following evidence in support of the Defense's motion:

- a. Charge Sheet.

LEGAL AUTHORITY AND ARGUMENT

5. The Defense submits that Section 793(e) has multiple unconstitutionally vague terms that render the statute unconstitutional. Additionally, Section 793(e) is substantially overbroad in violation of the First Amendment. In the alternative, if this Court does not find that Section 793(e) is either unconstitutionally vague or substantially overbroad, this Court should provide limiting instructions that narrow the breadth of Section 793(e) and more clearly define its vague terms.

A. 18 U.S.C. Section 793(e) is Unconstitutionally Vague in Violation of the Due Process Clause

6. As a general rule, "the void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." *Kolender v. Lawson*, 461 U.S. 352, 357 (1983); see *United States v. Moore*, 58 M.J. 466, 469 (C.A.A.F. 2003).

7. Among other requirements, the vagueness doctrine mandates that penal statutes provide fair warning of the conduct that is prohibited. *United States v. Lanier*, 520 U.S. 259, 265 (1997). The doctrine enshrines the principle "that no man shall be held criminally responsible for conduct which he could not reasonably understand to be proscribed" in three important respects. *Id.* at 265-66 (quoting *Bouie v. City of Columbia*, 378 U.S. 347, 351 (1964)). First, it "bars enforcement of 'a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its interpretation.'" *Id.* at 266 (quoting *Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926)). Second, the rule of lenity "ensures fair warning" by counseling courts to interpret an ambiguous statute to proscribe only "conduct clearly covered." *Id.* Third, although limited judicial gloss is permitted to clarify some uncertainty in a statute, that gloss must not be novel or so substantial as to constitute judicial rewriting of the statute; a court "may impose a limiting construction on a statute only if it is 'reasonably susceptible' to such a construction." *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 884 (1997); see *id.* at 884-85; *Lanier*, 520 U.S. at 266.

8. Section 793(e) punishes:

Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic

negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it[.]

18 U.S.C. § 793(e). The Defense submits that the phrases “relating to the national defense” and “to the injury of the United States or to the advantage of any foreign nation” are unconstitutionally vague. With these two vague phrases working in concert, Section 793(e) fails to provide the fair warning required by the Due Process Clause. Each unconstitutionally vague term is discussed in turn.

(1) The Phrase “Relating to the National Defense” is Unconstitutionally Vague

9. The phrase “relating to the national defense” is unconstitutionally vague because it gives no fair warning of what information comes within its sweeping scope. How close of a connection to national defense must the information have before it is “relating to the national defense?” Will any conceivable connection suffice? The language of Section 793(e) provides no answer, and courts have spent considerable time and effort in a vain attempt to give some content to this exceedingly vague phrase. See *United States v. Squillacote*, 221 F.3d 542, 576 (4th Cir. 2000) (“[Sections 793 and 794] unfortunately provide *no guidance* on the question of what kind of information may be considered related to or connected with the national defense. The task of defining ‘national defense’ information thus has been left to the courts.” (emphasis added)). In the meantime, members of the public “must necessarily guess at its meaning and differ as to its interpretation.” *Lanier*, 520 U.S. at 266 (quoting *Connally*, 269 U.S. at 391).

10. The first effort in the long line of cases interpreting this phrase was made by the United States Supreme Court in *Gorin v. United States*, 312 U.S. 19 (1941), in interpreting a predecessor statute. There, the Court held that the term “national defense” was a “generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness.” *Id.* at 28 (internal quotations omitted). It soon became clear, however, that this definition could not be the end of the matter. After all, “[t]here are innumerable documents referring to the military or naval establishments, or related activities of national preparedness, which threaten no conceivable security or other government interest that would justify punishing one who ‘communicates’ such documents.” Melville B. Nimmer, *National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case*, 26 Stan. L. Rev. 311, 326 (1974). The serious First Amendment implications if the *Gorin* Court’s interpretation were to be accepted for all cases could not be overlooked. Thus, the search for the ideal judicial gloss on this vague statutory term continued.

11. In *United States v. Heine*, 151 F.2d 813 (2d Cir. 1945), Judge Learned Hand attempted to provide this gloss. The court first explained the problem with the potentially all-encompassing

phrase “relating to the national defense”: “It seems plain that the [phrase] cannot cover information about all those activities which become tributary to ‘the national defense’ in time of war; for in modern war there are none which do not.” *Id.* at 815. Without providing a definitive gloss on what the phrase meant, the court settled on identifying information that was not included in that phrase, explaining that “[i]nformation relating to the national defense,” whatever else it means, cannot . . . include” information that the Government has itself made public. *Id.* at 816.

12. Since *Heine*, courts have continued to refine the notion of when information is sufficiently public to be outside Section 793(e) and when it is sufficiently “relating to the national defense.” The Fourth Circuit, for instance, has provided further judicial gloss on the phrase, requiring the information to be “closely held” by the Government and not lawfully available to the general public. *See United States v. Morison*, 844 F.2d 1057, 1071-72 (4th Cir. 1988) (approving district court’s instruction using this closely held language); *United States v. Dedeyan*, 584 F.2d 36, 39-40 (4th Cir. 1978) (similar).

13. This “closely held” gloss cannot in itself provide the requisite fair notice, however. Given the Government’s tendency over the years to over-classify information, *see, e.g.*, Reducing Over-Classification Act, Pub. L. No. 111-258, § 2(1), 124 Stat. 2648 (2010) (“security requirements nurture over-classification and excessive compartmentation of information among agencies”), classification of information is not a talisman indicating that the information is in fact closely held by the government. Through all of this judicial gloss and classification obfuscation, the only thing that remains clear about the phrase “relating to the national defense” is this: it cannot provide the constitutionally required fair warning of what information comes within its scope.

14. Heaping one limiting construction on top of another, courts have long struggled to provide by interpretation the requisite fair warning that the phrase “relating to the national defense” cannot supply on its own. These unsuccessful efforts demonstrate that the phrase is not reasonably susceptible to a limiting construction. *See Reno*, 521 U.S. at 884. Accordingly, as the phrase “relating to the national defense” fails to provide the fair warning required under the vagueness doctrine, it is unconstitutionally vague in violation of the Fifth Amendment to the United States Constitution.

(2) The Phrase “to the Injury of the United States or to the Advantage of Any Foreign Nation” is Unconstitutionally Vague

15. Additionally, the phrase “to the injury of the United States or to the advantage of any foreign nation” is unconstitutionally vague because it fails to provide a defendant with fair warning of what constitutes criminal conduct. This phrase runs afoul of the vagueness doctrine in three respects: its use of the disjunctive casts a wide net on the types of information covered; courts have transplanted the phrase from a modifier of information to a modifier of the requisite *mens rea*; and it fails to give any indication of what type or how much of a potential injury or advantage must exist before it is triggered.

16. The phrase “to the injury of the United States or to the advantage of any foreign nation” is phrased in the disjunctive. Thus, even where the United States suffers no injury, the phrase is

still potentially implicated. Given the potential First Amendment interests that may be at stake with respect to the disclosure of information, the phrase's broad scope is problematic. "[I]f a communication does not work an injury to the United States, it would seem to follow logically that no government interest can be asserted to overcome the first amendment's guarantee of freedom of speech." Nimmer, *supra*, at 330.

17. Moreover, in their attempt to provide content to the phrase through judicial gloss, courts have impermissibly transplanted the phrase to cure vagueness concerns presented by other phrases of Section 793(e). For example, at least two courts have used the "to the injury of the United States or to the advantage of any foreign nation" phrase to shore up the shoddy mens rea of Section 793(e) by holding that a combination of evil motive, bad or underhanded purpose, and acting with the intent to injure the United States is the necessary mens rea. See, e.g., *United States v. Truong Dinh Hung*, 629 F.2d 908, 918-19 (4th Cir. 1980); *United States v. Rosen*, 445 F. Supp. 2d 602, 625-26 (E.D. Va. 2006). The problem with this transplantation is that, under the statutory text, the phrase "to the injury of the United States or to the advantage of any foreign nation" modifies the type of information – "relating to the national defense" – not the state of mind of the accused. See 18 U.S.C. § 793(e) ("information relating to the national defense *which information* the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation" (emphasis added)). Moreover, the use of one vague term of a statute in an attempt to make a different vague term constitutionally clear is simply circular and is further evidence of Section 793(e)'s vagueness.

18. Finally, the statutory text gives no substance to the terms "injury" or "advantage." What type of injury or advantage is contemplated by Section 793(e)? What magnitude of injury or advantage is required? These questions lead to the ultimate question for vagueness purposes: How is a person supposed to know what conduct is proscribed by the statute when the statute itself leaves so many questions unanswered?

19. For these reasons, the phrase "to the injury of the United States or to the advantage of any foreign nation" is unconstitutionally vague.

(3) These Two Vague Phrases Render Section 793(e) Unconstitutionally Vague

20. The vague provisions mentioned above render Section 793(e) unconstitutionally vague. The precise meaning of each phrase has eluded the courts. In fact, no court has held that the plain statutory text has provided fair notice of what conduct is proscribed. Moreover, substantial judicial gloss has been unable to give clear content to these phrases. Where, as here, courts are forced to trade in the tools of statutory construction for the tools of legislative drafting in an attempt to remedy the rampant ambiguities of a criminal statute, the Due Process Clause of the Fifth Amendment has been offended.

21. The rule of lenity, one of the three manifestations of the fair warning requirement, requires that any ambiguity in a criminal statute be resolved in the accused's favor. See *Lanier*, 520 U.S. at 266. Because of the fatal ambiguities in Section 793(e), this Court should declare Section 793(e) unconstitutionally vague and dismiss Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II.

B. 18 U.S.C. Section 793(e) is Unconstitutionally Overbroad in Violation of the First Amendment

22. A law is substantially overbroad in violation of the First Amendment where “a substantial number of its applications are unconstitutional, judged in relation to the statute’s plainly legitimate sweep.” *United States v. Stevens*, ___ U.S. ___, 130 S. Ct. 1577, 1587 (2010) (quoting *Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 449 n.6 (2008)); see *City of Houston v. Hill*, 482 U.S. 451, 466-67 (1987).

23. The Defense submits that Section 793(e) is substantially overbroad in violation of the First Amendment. By its broad terms, Section 793(e) regulates a substantial amount of protected speech. Additionally, Section 793(e) infringes on the freedom of the press to investigate and publish articles on national defense topics.

24. Section 793(e) clearly regulates a wide range of speech: it prohibits any willful communication, delivery, transmission, retention (or attempt to commit any of these acts) of any information relating to the national defense, provided that the person has unauthorized possession and reason to believe that the information could be used to the injury of the United States or to the advantage of any foreign nation. See 18 U.S.C. § 793(e). Information relating to the national defense could include speech about government programs and policies, as well as public affairs – core political speech under the First Amendment. See *Connick v. Myers*, 461 U.S. 138, 145 (1983).

25. Moreover, Section 793(e) targets disclosure or retention of only information relating to the national defense; if the information does not relate to the national defense, the speech is not regulated under Section 793(e). Thus, Section 793(e) is a content-based regulation of speech. See *Stevens*, 130 S. Ct. at 1584; *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 642-43 (1994). Such content-based regulations of speech are “presumptively invalid, and the Government bears the burden to rebut that presumption.” *Stevens*, 130 S. Ct. at 1584 (quoting *United States v. Playboy Entm’t Group, Inc.*, 529 U.S. 803, 817 (2000)) (internal quotations omitted).

26. While the Government certainly has a strong interest in national security, the Government’s invocation of its national security interest cannot simply vitiate bedrock First Amendment protections. As Judge Wilkinson explained in his concurrence in *Morison*:

The First Amendment interest in informed popular debate does not simply vanish at the invocation of the words “national security.” National security is public security, not government security from informed criticism. No decisions are more serious than those touching on peace and war; none are more certain to affect every member of society. Elections turn on the conduct of foreign affairs and strategies of national defense, and the dangers of secretive government have been well documented.

844 F.2d at 1081. Justice Douglas sounded similar sentiments in his concurrence in *New York Times Co. v. United States*, 403 U.S. 713 (1971), stating that “[s]ecrecy in government is

fundamentally anti-democratic, perpetuating bureaucratic errors. Open debate and discussion of public issues are vital to our national health.” *Id.* at 724. Therefore, notwithstanding the Government’s interest in national security, the First Amendment interests implicated in information relating to the national defense are substantial and must not be overlooked.

27. Additionally, Section 793(e) poses substantial dangers to the free speech rights of reporters who investigate and publish stories on national defense related topics.¹ Under the terms of Section 793(e), if a reporter had unauthorized possession of information relating to the national defense and published a story containing that information, having reason to believe that the information in the story could be used to the injury of the United States or to the advantage of any foreign nation, that reporter could be subjected to criminal prosecution. *See* 18 U.S.C. § 793(e). If Section 793(e) is upheld, the chilling effect it will have on this core speech of public concern will be dramatic.

28. For these reasons, Section 793(e) is substantially overbroad in violation of the First Amendment. Accordingly, this Court should dismiss Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II.

C. In the Alternative, This Court Should Provide Limiting Instructions That Narrow the Breadth of Section 793(e) and More Clearly Define its Vague Terms

29. While the Defense maintains that, for the reasons articulated above, Section 793(e) is both unconstitutionally vague and substantially overbroad, in the event that this Court finds otherwise, the Defense requests this Court to provide limiting instructions that narrow the breadth of Section 793(e) and more clearly define its vague terms. Specifically, the Defense requests that the Court provide multiple limiting instructions for the term “relating to the national defense.”

30. In its definition of the term “relating to the national defense,” this Court should inform the members that the Government must prove beyond a reasonable doubt that the information at issue would be potentially damaging to the United States if disclosed. *See Morison*, 844 F.2d at 1071-72 (approving a jury instruction with this language). Moreover, the potential for the damage to national security if the information is disclosed must be reasonable and direct; a strained or distant likelihood of such harm is insufficient. *See Gorin*, 312 U.S. at 31 (approving a jury instruction with this language). Finally, the type of harm that disclosure of the information is likely to cause must be endangerment to “the environment of physical security which a functioning democracy requires.” *Morison*, 844 F.2d at 1082 (Wilkinson, J., concurring).

31. As this prosecution also implicates First Amendment concerns, this Court should instruct the members that the Government must prove beyond a reasonable doubt that “potentially damaging to the United States” means that a disclosure of the information would be likely to cause

¹ Though PFC Manning is not a reporter or member of the news media, he is permitted to assert their rights in an overbreadth challenge to a statute on First Amendment grounds. *See United States v. Bilby*, 39 M.J. 467, 468-69 n.2 (C.M.A. 1994) (“First Amendment overbreadth is one of the few exceptions to the principle that ‘a person to whom a statute may constitutionally be applied may not challenge that statute on the ground that it may conceivably be applied unconstitutionally to others in situations not before the Court.’” (quoting *New York v. Ferber*, 458 U.S. 747, 767 (1982))).

imminent serious injury to the United States. See *New York Times*, 403 U.S. at 726-27 (Brennan, J., concurring); Nimmer, *supra*, at 331-32.

32. Additionally, this Court should further instruct the members that on the "relating to the national defense" element the Government must prove beyond a reasonable doubt that the Government closely held the information and that the accused knew the information was closely held. See *Morison*, 844 F.2d at 1071-72 (approving district court's instruction using this closely held language); *Dedeyan*, 584 F.2d at 39-40 (similar); *Rosen*, 445 F.Supp.2d at 620, 625 (discussing closely held requirement and requirement of accused's knowledge that the information was closely held). To do this, the Government must prove at least two things: (1) that the information was classified and (2) that the information was not otherwise available to the public.

CONCLUSION

33. For these reasons, the Defense requests this Court to dismiss Specification 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II because Section 793(e) is unconstitutionally vague in violation of the Fifth Amendment and substantially overbroad in violation of the First Amendment. In the alternative, the Defense requests this Court to provide limiting instructions that narrow the breadth of Section 793(e) and more clearly define its vague terms.

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel



JOSHUA J. TOOMAN
CPT, JA
Defense Counsel

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

GOVERNMENT RESPONSE
TO DEFENSE MOTION TO
DISMISS SPECIFICATIONS
2, 3, 5, 7, 9, 10, 11, AND 15
OF CHARGE II

24 May 2012

RELIEF SOUGHT

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny the defense motion to dismiss Specifications 2, 3, 5, 7, 9, 10, 11, and 15 of Charge II. 18 U.S.C. § 793(e) is neither unconstitutionally vague in violation of the Fifth Amendment to the United States Constitution, nor substantially overbroad in violation of the First Amendment.

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the defense has the burden of persuasion on any factual issue the resolution of which is necessary to decide the motion. *Manual for Courts-Martial (MCM), United States*, Rule for Courts-Martial (RCM) 905(c)(2) (2008). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

FACTS

The United States stipulates to the facts as set forth in the defense motion.

WITNESSES/EVIDENCE

The United States requests this Court consider the referred charge sheet in support of its response to the defense motion.

LEGAL AUTHORITY AND ARGUMENT

The defense argues that 18 U.S.C. § 793(e) is unconstitutionally vague on its face in violation of the Fifth Amendment because the phrases "relating to the national defense" and "to the injury of the United States or to the advantage of any foreign nation" do not provide the fair warning required by the Due Process Clause. Def. Mot. at 3. Additionally, the defense argues that 18 U.S.C. 793(e) is substantially overbroad in violation of the First Amendment because it "regulates a substantial amount of protected speech" and "infringes on the freedom of the press

to investigate and publish articles on national defense topics.” Def. Mot. at 6. The defense arguments have no merit for the reasons set forth below.

I. THE DEFENSE SHOULD BE PRECLUDED FROM CHALLENGING 18 U.S.C. § 793(e) AS VAGUE ON ITS FACE.

At the outset, the defense should be precluded from mounting a facial vagueness challenge to 18 U.S.C. § 793(e), rather than an as-applied challenge, because there are no First Amendment rights implicated in this case. See *United States v. Mazurie*, 419 U.S. 544, 550 (1975) (“It is well established that vagueness challenges to statutes which do not involve First Amendment freedoms must be examined in the light of the facts of the case at hand.”). First Amendment cases are different and are “concerned with the vagueness of the statute ‘on its face’ because such vagueness may in itself deter constitutionally protected and socially desirable conduct.” *United States v. National Dairy Products Corp.*, 372 U.S. 29, 36 (1963); *United States v. Sun*, 278 F.3d 302, 309 (4th Cir. 2002).

Although it is unclear whether a First Amendment issue can ever arise in a prosecution under the Espionage Act, the Fourth Circuit, considering a vagueness challenge to § 793(d) and (e) in a leak case involving a naval intelligence employee, stated “Actually we do not perceive any First Amendment rights to be implicated here.” *United States v. Morison*, 844 F.2d 1057, 1068 (4th Cir. 1988). Similarly, in *United States v. Kim*, the court rejected a defendant’s First Amendment challenge in a prosecution for oral disclosures of classified information. *United States v. Kim*, 808 F. Supp. 2d 44, 56-57 (D.D.C. 2011). The court ultimately held that for purposes of the First Amendment, there was no difference between oral disclosures and written disclosures of classified information. *Id.* at 56. Further, the court noted the uniformly held view that government employees who sign security agreements lack protection under the First Amendment. *Id.* at 57 (citing *McGehee v. Casey*, 718 F.2d 1137, 1143 (D.C. Cir. 1983); *Bernsten v. CIA*, 618 F. Supp. 2d 27, 29 (D.D.C. 2009)); see also *Morison*, 844 F.2d at 1070 (“[W]hen [§ 793(e)] is applied to a defendant in the position of the defendant here, there is no First Amendment right implicated.”).

The accused in this case is charged with multiple specifications alleging willful communication of national defense information to unauthorized persons. The evidence will show that the accused signed multiple non-disclosure agreements. Accordingly, no First Amendment rights are implicated by application of 18 U.S.C. § 793(e) to the conduct in this case. The defense should be precluded from asserting a facial vagueness challenge to the statute.

II. 18 U.S.C. § 793(e) PROVIDES THE FAIR WARNING REQUIRED BY THE DUE PROCESS CLAUSE.

Assuming, *arguendo*, First Amendment rights are implicated in this case, 18 U.S.C. § 793(e) is not unconstitutionally vague because it provides fair warning to persons of ordinary intelligence. In particular, the phrase “related to the national defense” has been repeatedly challenged by defendants on the basis of impermissible vagueness and has survived the scrutiny

of the Supreme Court and multiple jurisdictions. See discussion *infra* Part II.A. While the defense motion does an adequate job summarizing the evolution of case law in this area, the defense has failed to distinguish this case from all the other cases that have considered 18 U.S.C. § 793(e) and related provisions and found the statute to be sufficiently definite.¹

A. The Phrase “Relating to the National Defense” is not Unconstitutionally Vague.

Due process requires that a statute be declared void when it “fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.” *United States v. Williams*, 553 U.S. 285, 304 (2008) (citing *Hill v. Colorado*, 530 U.S. 703, 732 (2000)). There is a strong presumption of validity that attaches to an Act of Congress; hence, “statutes are not automatically invalidated as vague simply because difficulty is found in determining whether certain marginal offenses fall within their language.” *Jordan v. De George*, 341 U.S. 223, 231 (1951); see also *Williams*, 553 U.S. at 305 (“Its basic mistake lies in the belief that the mere fact that close cases can be envisioned renders a statute vague.”). Clarity at the requisite level may be supplied by judicial gloss on an otherwise uncertain statute. See *United States v. Lanier*, 520 U.S. 259, 266 (1997).

The defense argues that the phrase “relating to the national defense” is unconstitutionally vague because it fails to give fair warning of “what information comes within its sweeping scope.” Def. Mot. at 3. However, every court that has had occasion to consider the phrase in the vagueness context has rejected the argument. In *Gorin v. United States*, 312 U.S. 19 (1941), the Supreme Court considered the same phrase in § 2(a) of the Espionage Act (the predecessor to § 793). The Court found the term “national defense” had a “well understood connotation” and held that the “language employed [in § 2(a)] appears sufficiently definite to apprise the public of prohibited activities and is consonant with due process.” *Id.* at 28. The defense motion makes no attempt to distinguish the holding in *Gorin* from this case.

Since the Supreme Court’s decision in *Gorin*, no other court has found the phrase “relating to the national defense” unconstitutionally vague in any context, specifically in cases involving charges under § 793. See *Morison*, 844 F.2d at 1071-74 (rejecting vagueness challenge and upholding the language of § 793(d) and (e)); *United States v. Dedeyan*, 584 F.2d 36, 39 (4th Cir. 1978) (rejecting vagueness challenge and upholding the language of § 793(f)); *United States v. Boyce*, 594 F.2d 1246, 1252 n.2 (9th Cir. 1979) (upholding the language of §§ 793 and 794); *United States v. Rosen*, 445 F. Supp. 2d 602, 617-22 (E.D. Va. 2006) (rejecting vagueness challenge and upholding the language of § 793(d) and (e)); *Kim*, 808 F. Supp. 2d at 53 (rejecting vagueness challenge and upholding the language of § 793(d)).

While it is true, as the defense notes, that the Fourth Circuit has provided further judicial gloss on the phrase “relating to the national defense,” the defense fails to establish why further refinement cannot remedy the vagueness concerns of language the Supreme Court considered

¹ 18 U.S.C. § 793(e) provides that “[w]hoever having unauthorized possession of...information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted...the same to any person not entitled to receive it...[s]hall be fined under this title or imprisoned not more than ten years, or both. 18 U.S.C. § 793(e).

"sufficiently definite" without judicial gloss. *Gorin*, 312 U.S. at 28; see also *Lanier*, 520 U.S. at 266 (noting that "clarity at the requisite level may be supplied by judicial gloss on an otherwise uncertain statute"); *Morison*, 844 F.2d at 1071 ("[A]ll vagueness may be corrected by judicial construction which narrows the sweep of the statute within the range of reasonable certainty."). In fact, the Fourth Circuit recently noted that the judicial glosses refining the meaning of "related to the national defense" arguably offer "more protection to defendants than required by *Gorin*." *United States v. Squillacote*, 221 F.3d 542, 580 n.23 (4th Cir. 2000). Finally, the defense makes no attempt to assert that these judicial glosses are inconsistent in any way, except to say that the "precise meaning of [the] phrase has eluded the courts." Def. Mot. at 5. Refinement through judicial gloss does not mean indecision or inconsistency, which might provide support for the defense position. Accordingly, this Court should find the phrase "relating to the national defense" sufficiently definite to overcome any claim of unconstitutional vagueness in violation of the Fifth Amendment.

B. The Phrase "to the Injury of the United States or to the Advantage of Any Foreign Nation" is not Unconstitutionally Vague.

The defense also argues that the phrase "to the injury of the United States or to the advantage of any foreign nation" is unconstitutionally vague. Def. Mot. at 4. While the United States is unaware of any case that challenges this specific phrase as unconstitutionally vague, courts have held that the phrase "reason to believe could be used to the injury of the United States or to the advantage of any foreign nation" is an additional *mens rea* requirement in cases where the accused is charged with disclosures of intangible information, such as oral disclosures of classified information. See *Rosen*, 445 F. Supp. 2d at 627 ("[A]dded scienter requirement is yet another ground for rejecting the defendants' vagueness challenge here."); see also *Kim*, 808 F. Supp. 2d at 51 (discussing Congress' decision to impose a *mens rea* requirement for the communication of "information"); 18 U.S.C. § 793(e). The phrase, when read with the words immediately preceding it in the statute ("reason to believe could be used"), is more accurately characterized as a limiting factor, rather than as a phrase inviting uncertainty as to its scope.

In any event, the phrase does not render § 793(e) unconstitutionally vague because of the other limitations of the statute. In particular, the statute requires the United States to prove the accused "willfully" communicated national defense information. 18 U.S.C. § 793(e). Thus, the United States must establish beyond a reasonable doubt that the accused had "knowledge that the conduct [at issue] was unlawful." *Bryan v. United States*, 524 U.S. 184, 191-92 (1998). The Supreme Court has repeatedly recognized that "a scienter requirement may mitigate a law's vagueness, especially with respect to the adequacy of notice to the complainant that his conduct is proscribed." *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 499 (1982); see also *Gonzales v. Carhart*, 550 U.S. 124, 149 (2007) ("[S]cienter requirements alleviate vagueness concerns."). Indeed, this Court held that a "knowing" scienter requirement "mitigates a law's vagueness especially with respect to actual notice of the conduct proscribed." Court's Ruling, dated 26 April 2012 (citing *United States v. Moyer*, 2012 WL 639277 (3rd Cir. 2012)). Moreover, the Supreme Court has held that a willfulness scienter requirement substantially undercuts any vagueness challenge to a statute's other terms. See *United States v. Ragen*, 314 U.S. 513, 524 (1942). But more importantly for the purposes of this case, the Fourth Circuit has relied on the "willfulness" scienter requirement in § 793(d) to reject a vagueness

challenge to that provision. See *Morison*, 844 F.2d at 1071; see also *Gorin*, 312 U.S. at 27-28 (rejecting vagueness challenge based on scienter requirement in statute); *Kim*, 808 F. Supp. 2d at 54 (“Because the Government must prove that Defendant knew his conduct was unlawful, he cannot complain that he did not have fair warning that he could be criminally prosecuted for his actions.”). In short, even if there are legitimate vagueness concerns with respect to the phrase “to the injury of the United States or to the advantage of any foreign nation,” they are negated by the willfulness requirement of § 793(e).

III. 18 U.S.C. § 793(e) IS NOT SUBSTANTIALLY OVERBROAD IN VIOLATION OF THE FIRST AMENDMENT.

A law may be invalidated as overbroad under the First Amendment if “a substantial number of its applications are unconstitutional, judged in relation to the statute’s plainly legitimate sweep.” *United States v. Stevens*, 130 S. Ct. 1577, 1587 (2010) (quoting *Washington State Grange v. Washington State Republican Party*, 522 US 442, 449 n.6 (2008)). The overbreadth doctrine is an exception to the generally applicable rules regarding facial challenges, in that it allows a defendant to raise the First Amendment rights of third parties whose “constitutionally protected speech may be ‘chilled’ by the specter of the statute’s punishment.” *Rosen*, 445 F. Supp. 2d at 642 (citing *Virginia v. Hicks*, 539 U.S. 113, 118-19 (2003)). “Invalidation for overbreadth is ‘strong medicine’ that is not to be ‘casually employed.’” *Williams*, 553 U.S. at 293 (quoting *Los Angeles Police Dep’t v. United Reporting Publishing Corp.*, 528 U.S. 32, 39 (1999)). As such, “[t]he first step in overbreadth analysis is to construe the challenged statute; it is impossible to determine whether a statute reaches too far without first knowing what the statute covers.” *Williams*, 553 U.S. at 293. A statute should be construed to avoid constitutional problems, if possible. See *United States v. Ferber*, 458 U.S. 747, 769 n.24 (1982).

The defense argues that 18 U.S.C. § 793(e) is substantially overbroad because it “regulates a wide range of speech.” Def. Mot. at 6. However, it is not enough to say that a statute applies broadly. In order for a statute to be invalidated as overbroad, the applications must be unconstitutional and they must be judged in comparison to the legitimate applications. See *Stevens*, 130 S. Ct. at 1587; *Rosen*, 445 F. Supp. 2d at 643. Like the defense assertion of impermissible vagueness, § 793 has endured similar challenges on the basis of substantial overbreadth. See *Rosen*, 445 F. Supp. 2d at 643; *Morison*, 844 F.2d at 1076. The court in *Rosen*, using the analysis discussed above, construed various terms and provisions of § 793(d) and (e) and ultimately concluded that the statute was “narrowly and sensibly tailored to serve the government’s legitimate interest in protecting the national security,” and judged its effect on First Amendment freedoms as “neither real nor substantial” in relation to the statute’s legitimate sweep. *Rosen*, 445 F. Supp. 2d at 643. Similarly, the court in *Morison* held that there was no fatal overbreadth with respect to the terms “national defense” and “one not entitled to receive,” as courts had narrowed the constructions of those terms. See *Morison*, 844 F.2d at 1076.


The defense also argues that § 793(e) “poses substantial dangers to the free speech rights of reporters who investigate and publish stories on national defense related topics.” Def. Mot. at 7. The concern is that a reporter could be subjected to criminal prosecution under the statute if

the United States proves every element of the statute beyond a reasonable doubt. See Def. Mot. at 7. Aside from the fact that § 793(e)'s effect on First Amendment rights has been judged neither real nor substantial, the Supreme Court tacitly approved such an application of § 793(e) in *New York Times Co. v. United States*, 403 U.S. 713—the “Pentagon Papers” case. See *Rosen*, 445 F. Supp. 2d at 638-39.


In *Rosen*, the defendants were employed by the American Israel Public Affairs Committee as lobbyists and were charged with conspiring to transmit information relating to the national defense to those not entitled to receive it, in violation of 18 U.S.C. § 793(g). *Id.* at 607-08. The *Rosen* defendants argued that the First Amendment bars Congress from punishing persons for disclosure of national defense information when they do not have a special relationship with the government. *Id.* at 637. In considering the contention, the *Rosen* court discussed the concurring opinions of Justices Stewart, White, and Marshall in the “Pentagon Papers” case. *Id.* at 638. While the Supreme Court was confronted with significant First Amendment issues raised by their consideration of the constitutionality of a prior restraint on the press, and ultimately denied the United States’ request for an injunction preventing the New York Times and Washington Post from publishing the contents of the “Pentagon Papers,” the *Rosen* court noted that the concurring opinions explicitly acknowledged the viability of a prosecution of the newspapers under applicable criminal law. *Id.*; see *New York Times Co.*, 403 U.S. at 730 (Stewart, J., concurring); *id.* at 737 (White, J., concurring); *id.* at 745 (Marshall, J., concurring). As such, the defense argument – that § 793(e) is fatally overbroad because it potentially permits the criminal prosecution of a reporter – is without merit. At most, overbreadth may be an issue when the statute is applied to a certain set of facts, but the hypothetical itself does not render § 793(e) substantially overbroad. See *Williams*, 553 U.S. at 303 (“The ‘mere fact that one can conceive of some impermissible applications of a statute is not sufficient to render it susceptible to an overbreadth challenge.’”) (quoting *Members of City Council of Los Angeles v. Taxpayers for Vincent*, 466 U.S. 789, 800 (1984)). Thus, for the reasons stated above, 18 U.S.C. § 793(e) is not substantially overbroad in violation of the First Amendment.

CONCLUSION

The United States respectfully requests this Court DENY the defense motion to dismiss Specifications 2, 3, 5, 7, 9, 10, 11, and 15 of Charge II. For the reasons stated above, 18 U.S.C. § 793(e) is neither unconstitutionally vague in violation of the Fifth Amendment, nor substantially overbroad in violation of the First Amendment. Additionally, the United States joins the defense in their request to provide instructions that further define 18 U.S.C. § 793(e), but requests that the Court adhere to the Scheduling Order dated 25 April 2012, which provides for litigation concerning proposed members instructions in phase 3a.


JODEAN MORROW
CPT, JA
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 24 May 2012.


JODEAN MORROW
CPT, JA
Trial Counsel

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, xxx-xx-[REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

**DEFENSE MOTION TO
DISMISS FOR FAILURE TO
STATE AN OFFENSE:
SPECIFICATIONS 13 AND 14
OF CHARGE II**

DATED: 10 May 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 907(b)(1)(B), requests this Court to dismiss Specifications 13 and 14 of Charge II because the Government has failed to allege that PFC Manning's alleged conduct exceeded authorized access within the meaning of 18 U.S.C. Section 1030(a)(1).

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. The Defense, as the moving party, bears the burden of this motion by a preponderance of the evidence pursuant to R.C.M. 905(c)(1)-(2)(A). "A charge or specification shall be dismissed at any stage of the proceedings if: (A) [t]he court-martial lacks jurisdiction to try the accused for the offense; or (B) [t]he specification fails to state an offense." R.C.M. 907(b)(1).

FACTS

3. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of conduct prejudicial to good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting government property, and two specifications of knowingly exceeding authorized access to a government computer, in violation of Articles 92, 104, and 134, Uniform Code of Military Justice (UCMJ) 10 U.S.C. §§ 892, 904, 934 (2010).

4. In Specification 13 of Charge II, the Government pleads that PFC Manning

did, at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, having knowingly exceeded authorized access on a Secret Internet Protocol Router Network computer, and by

means of such conduct having obtained . . . more than seventy-five classified United States Department of State cables, willfully communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted the said information, to a person not entitled to receive it, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, in violation of 18 U.S. Code Section 1030(a)(1)[.]

Charge Sheet (attached), Specification 13. Specification 14 of the same charge alleges that PFC Manning

did, at or near Contingency Operating Station Hammer, Iraq, between on or about 15 February 2010 and on or about 18 February 2010, having knowingly exceeded authorized access on a Secret Internet Protocol Router Network Computer, and by means of such conduct having obtained . . . a classified Department of State cable titled "Reykjavik-13", willfully communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted the said information, to a person not entitled to receive it, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, in violation of 18 U.S. Code Section 1030(a)(1)[.]

Id., Specification 14. In its Bill of Particulars, the Defense asked the Government to specify how exactly it alleges that PFC Manning exceeded authorized access. The Government resisted providing these particulars. However, during the motions argument, CPT Morrow revealed the Government's position on how PFC Manning is alleged to have exceeded authorized access:

MJ: Okay. Government, do you have a theory of a means by which he knowingly exceeded the unauthorized [sic] access?

ATC1: The means?

MJ: Yes.

ATC1: Your Honor, the government would maintain that PFC Manning had a user name and a password to a SIPRNET computer while deployed. On certain occasions when he accessed that computer for certain, you know, to obtain these documents, he was exceeding authorized access. I can't -- there is no means. I mean, there is no -- I don't think it's -- a mystery how he got onto the computer. I think Mr. Coombs is focusing on the [inaudible] diplomacy aspect of it when the focus should be on when he access [sic] the computer to do certain things.

MJ: So your means is the fact that he accessed the computer to do certain things?

ATC1: Yes, ma'am.

MJ: All right. Are those things that he did part of the investigation or he --

ATC1: They are part of the specification, Your Honor. Obtaining these cables and transmitting to Wikileaks.

Oral Argument, Unauthenticated Transcript, 23 February 2012, pp. 71-72 [hereinafter Oral Argument, Unauthenticated Transcript].

WITNESSES/EVIDENCE

5. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this court to consider the following evidence in support of the Defense's motion:

- a. Charge Sheet (attached);
- b. Oral Argument, Unauthenticated Transcript, 23 February 2012.

LEGAL AUTHORITY AND ARGUMENT

6. To state an offense under 18 U.S.C. Section 1030(a)(1), the Government must allege that the accused either knowingly accessed a computer without authorization or that he knowingly exceeded authorized access in accessing the information in question. The Government in this case has alleged that PFC Manning knowingly exceeded his authorized access when, despite being authorized to use the computer, he accessed certain information for an improper purpose and/or in violation of the governing terms of use, and disclosed the information to a person not authorized to receive it.

7. The plain language of Section 1030(e)(6) clearly indicates that a person exceeds authorized access when he or she uses authorized access to a computer to obtain or alter information in the computer that he or she is not entitled to obtain or alter. 18 U.S.C. § 1030(e)(6). Neither Section 1030(e)(6) nor Section 1030(a)(1) gives any indication that an accused's purpose in accessing the computer or the information in question is in any way relevant to the "exceeding authorized access" inquiry. *See id.* § 1030(a)(1), (e)(6). It is clear from the plain language of Section 1030(a)(1) that PFC Manning did not exceed authorized access within the meaning of the statute. PFC Manning had full authority to access the government computer(s) at issue and at no time did he obtain or alter information that he was not entitled to obtain or alter.

8. The essence of the Government's theory is either: a) that PFC Manning exceeded authorized access when he allegedly accessed information for an improper purpose, *viz.*, to give the information to someone not authorized to receive it; or b) that PFC Manning exceeded authorized access when he allegedly accessed, stored and disclosed information in contravention of the Army's Acceptable Use Policy (AUP).¹ Either way, the Government fails to state an

¹ This latter theory was presented by the Government at the Article 32 hearing.

offense under Section 1030(a)(1).² Under Section 1030(a)(1), an accused's purpose in accessing the computer is irrelevant, as is the question of whether the accused violated the employer's terms of use. The inquiry under Section 1030(a)(1) is strictly limited to whether the accused had authority to access the information accessed. Other sections of federal criminal law or the UCMJ may criminalize PFC Manning's alleged improper storing or dissemination of information – but not Section 1030(a)(1).

9. Additionally, interpreting the term “exceeds authorized access” to include instances where a person accesses information for an improper purpose or where a person violates the terms of use of that access poses serious constitutional concerns for at least one provision of the statute.³ Therefore, this expansive interpretation must be rejected.

10. Because the Government has failed to allege that PFC Manning “exceeded authorized access” within the meaning of Section 1030(a)(1), the charge should be dismissed for failure to state an offense.

A. Under the Plain Language of 18 U.S.C. Section 1030(a)(1), PFC Manning Did Not Exceed His Authorized Access

11. As outlined in *United States v. Starr*, the proper inquiry regarding the legal meaning of a statute is as follows:

It is the function of the legislature to make the laws and the duty of judges to interpret them. 2A Norman J. Singer, *Sutherland Statutory Construction* § 45.03 (4th ed. 1984). Judges should interpret a statute so as to carry out the will of the legislature. *United States v. Dickenson*, 20 C.M.R. 154, 165 (C.M.A. 1955). Otherwise, they violate the principle of the separation of powers. Singer, *supra*, § 45.05. “If the words used in the statute convey a clear and definite meaning, a court has no right to look for or to impose a different meaning.” *Dickenson*, 20 C.M.R. at 165. Thus, in interpreting a statute, we employ the following process: (1) Give the operative terms of the statute their ordinary meaning; if the terms are unambiguous, the inquiry is over; (2) If the operative terms of the statute are

² If the Government claims, as it did with the Motion to Dismiss the Article 104 Offense, that the charges should not be dismissed because the specification is sufficient, the Defense would like to clarify that its argument is not that the specification is deficient; it is that the theory underlying the specification is deficient. This is appropriately styled as a motion to dismiss for failure to state an offense. See, e.g., *United States v. Nosal* (*Nosal III*), ___ F.3d ___, No. 10-10038, 2012 WL 1176119, at *8 (9th Cir. April 10, 2012) (en banc) (holding that the district court's dismissal of the counts of the indictment alleging violations of Section 1030 was proper because the Government's theory of “exceeds authorized access” was erroneous).

³ The term “exceeds authorized access” or some derivative thereof appears in several provisions of Section 1030. See, e.g., 18 U.S.C. § 1030(a)(1) (“exceeding authorized access”); *id.* § 1030(a)(2) (“exceeds authorized access”); *id.* § 1030(a)(4) (same); *id.* § 1030(a)(7)(B) (“in excess of authorization” and “exceeding authorized access”). These phrases are nearly identical and “identical words and phrases within the same statute should normally be given the same meaning.” *Nosal III*, 2012 WL 1176119, at *4 (quoting *Powerex Corp. v. Reliant Energy Servs., Inc.*, 551 U.S. 224, 232 (2007)) (internal quotations omitted). Thus, the interpretation of the term “exceeds authorized access” contained in Section 1030(e)(6) applies to all variants of the term used, including “exceeding authorized access” in Section 1030(a)(1). See *id.* (“Congress obviously meant ‘exceeds authorized access’ to have the same meaning throughout [S]ection 1030.”).

ambiguous, then we examine the purpose of the statute as well as its legislative history; and (3) If a reasonable ambiguity still exists, then we apply the rule of lenity and resolve the ambiguity in favor of the accused. See *United States v. Ferguson*, 40 M.J. 823, 830 (N.M.C.M.R. 1994).

51 M.J. 528, 532 (A.F. Ct. Crim. App. 1999); see also *United States v. McGuinness*, 33 M.J. 781, 784-85 (N.M.C.M.R. 1991) ("First, a court should give all the terms used in the statute their ordinary meaning. Second, if a possible ambiguity exists in the statute when a term's ordinary meaning is used, then a court must examine the legislative history and motivating policies of Congress in enacting the statute to resolve the ambiguity. And finally, if after applying steps one and two, a reasonable doubt still exists about a statute's intended scope, then the Court will apply the rule of lenity and resolve the ambiguity in favor of the appellant.").

12. The term "exceeds authorized access" in Section 1030 has a clear legal meaning. A person exceeds authorized access under Section 1030(a)(1) when, despite being authorized to use the computer, the accused uses his access to the computer to obtain or alter information in the computer that he is not entitled to obtain or alter. Section 1030 is thus concerned only with bypassing technical restrictions on access, not the improper purpose for which one has accessed the information. Alternatively, if this Court determines that the statutory language is ambiguous (which the Defense believes it is not), then the purpose of the statute and the legislative history clearly indicate that Section 1030 was not intended to address misuse of information, only misuse of the computer, in the sense of hacking or bypassing technical restrictions. If, after a review of the plain language and legislative history, the Court concludes that there is still ambiguity, then that ambiguity must be resolved in favor of the accused under the rule of lenity.

13. Section 1030(a)(1) punishes:

Whoever --

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government . . . to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . . with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it[.]

18 U.S.C. § 1030(a)(1). In this case, the Government has proceeded under the theory that PFC Manning knowingly exceeded his authorized access in accessing certain information and disclosing that information to persons not authorized to receive it, in contravention of the Government's Acceptable Use Policy and/or that PFC Manning accessed information for an improper purpose. Notably, the Government has not alleged that PFC Manning accessed a

computer that he was not entitled to access. Nor has the Government alleged that PFC Manning accessed information on the computer that he was not entitled to access.

14. Congress has provided a definition for “exceeds authorized access” in Section 1030(e)(6): “the term ‘exceeds authorized access’ means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter[.]” *Id.* § 1030(e)(6).⁴ This language is plain and unambiguous. *See United States v. Inthavong*, 48 M.J. 628, 630 (A. Ct. Crim. App. 1998) (“[S]tatutory ambiguity may not be manufactured as a device to defeat manifest congressional intent.”). An accused exceeds authorized access under Section 1030(a)(1) when, despite being authorized to use the *computer*, the accused uses his access to the computer to obtain or alter *information* in the computer that he is not entitled to obtain or alter.

15. For instance, if PFC Manning had used his government computer (to which he has authorized access) to hack into the White House server and obtain President Obama’s official e-mails, he would presumably be “exceeding authorized access.” Likewise, if PFC Manning had used his government computer (to which he has authorized access) to change the contents of diplomatic cables on the server, he would be “exceeding authorized access.” In short, the section is intended to punish those who, while authorized to use the computer, bypass technical restrictions and use the computer to access or alter information that they are not allowed to access or alter. The section does not extend to the situation where the user has authorization to access the information in question, but somehow misuses or misappropriates that information. *See United States v. Nosal (Nosal III)*, ___ F.3d ___, No. 10-10038, 2012 WL 1176119, at *7-8 (9th Cir. April 10, 2012) (en banc); *United States v. Aleynikov*, 737 F. Supp. 2d 173, 192 (S.D.N.Y. 2010); *Orbit One Commc’ns, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) (“The plain language of [Section 1030] supports a narrow reading. [Section 1030] expressly prohibits improper ‘access’ of computer information. It does not prohibit misuse or misappropriation.”); *see also Xcedex, Inc. v. VMware, Inc.*, No. 10-3589 (PJS/JJK), 2011 WL 2600688, at *4 (D. Minn. June 8, 2011) (“[Section 1030] itself defines ‘exceeds authorized access’ as ‘access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.’ 18 U.S.C. § 1030(e)(6). Therefore, ‘without authorization’ and ‘exceed[ing] authorized access’ depend on the ‘unauthorized use of access,’ not on the ‘unauthorized use of information.’” (emphasis in original)); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (“[T]he plain language of [Section] 1030(a)(2), (4), and (5)(A)(iii) target ‘the unauthorized procurement or alteration of information, not its misuse or misappropriation.’”).

16. PFC Manning clearly had authorization to access the government computers in question.

⁴ Section 1030(a)(1) today uses the phrase “exceeding authorized access” instead of “exceeds authorized access.” 18 U.S.C. § 1030(a)(1). This subsection was amended in 1996 by substituting the term “exceeding” for the term “exceeds,” which had been used in that subsection since 1986. *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, § 201(1)(A)(ii), 110 Stat. 3488, 3491. The change in phrasing was likely grammatical only and the definition of “exceeds authorized access” in Section 1030(e)(6) is likely still applicable to the term “exceeding authorized access” in Section 1030(a)(1). *See* S. Rep. 104-357 (1996) (“The amendment specifically covers the conduct of a person who deliberately breaks into a computer without authority, or an insider who *exceeds authorized access*, and thereby obtains classified information and then communicates the information to another person, or retains it without delivering it to the proper authorities.” (emphasis supplied)).

Thus, the only remaining question is whether the Government alleges that PFC Manning “exceed[ed] authorized access” within the meaning of Section 1030 – i.e. whether he “obtain[ed] or alter[ed] information in the computer that [he was] not entitled so to obtain or alter[.]” 18 U.S.C. § 1030(e)(6). The Government has not alleged that PFC Manning used his access to obtain information that he was not entitled to obtain. On the contrary, the Government will concede that PFC Manning was authorized to obtain each and every piece of information that he allegedly accessed. Similarly, the Government has not alleged that PFC Manning altered any of the information that he allegedly accessed. Instead, the Government alleges that because PFC Manning had an improper purpose in accessing the information that he had full permission to access, he has exceeded authorized access within the meaning of the statute. This is an incorrect reading of the term “exceeds authorized access” – and one which conflicts with the plain meaning of the statute. See *Walsh Bishop Assocs., Inc. v. O’Brien*, No. 11-2673 (DSD/AJB), 2012 WL 669069, at *3 (D. Minn. Feb. 28, 2012) (“The language of [Section] 1030(a)(2) does not support the interpretation of Walsh Bishop. Instead, Walsh Bishop’s interpretation requires the court to rewrite the statute to replace the phrase ‘to use such access to obtain or alter information that the accessor is not entitled so to obtain or alter’ with ‘to use such information in a manner that the accessor is not entitled so to use.’ But subsection (a)(2) is not based on use of information; it concerns access. Indeed, the language of subsection (a)(1) shows that Congress knows how to target the use of information when it intends to do so.”); *United States v. Zhang*, No. CR-05-00812 RMW, 2010 WL 4807098, at *3 (N.D. Cal. Nov. 19, 2010) (“Nonetheless, a plain reading of [S]ection 1030(e)(6)’s definition . . . compels a different conclusion. An individual ‘exceeds authorized access’ if he or she has permission to access a portion of the computer system but uses that access to ‘obtain or alter information in the computer that [he or she] is not entitled so to obtain or alter.’ As the court in *Norsal* [sic] explained, ‘there is simply no way to read that definition to incorporate policies governing use of information unless the word alter is interpreted to mean misappropriate.’” (citations omitted)).

17. The plain language of “exceeds authorized access” is further supported by looking at the specification itself. The Government alleges:

In that Private First Class Bradley E. Manning, U.S. Army, did, at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, having knowingly *exceeded authorized access* on a Secret Internet Protocol Router Network computer, *and by means of such conduct having obtained information* that has been determined by the United States government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, to wit: more than seventy-five classified United States Department of State cables[.]

Charge Sheet, Specification 13 (emphasis supplied). It is clear that “exceeding authorized access” is different from, and a predicate to, “obtaining information.” If the term “exceeded authorized access” is interpreted as the Government suggests, the charge would be redundant and nonsensical:

In that Private First Class Bradley E. Manning, U.S. Army, did, at or near

Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, having knowingly [“accessed that computer ... to obtain these documents,” see Oral Argument, Unauthenticated Transcript, *supra*] on a Secret Internet Protocol Router Network computer, and by means of such conduct having obtained information that has been determined by the United States government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, to wit: more than seventy-five classified United States Department of State cables[.]

Charge Sheet, Specification 13 (alteration supplied). Thus read, the charge does not make sense since “exceeding authorized access” is conflated with obtaining documents for an improper purpose, which is the next part of the charge (“by means of such conduct having obtained information”). Thus, the exceeding authorized access cannot be the same as “obtain[ing] information” or the specification falls apart. This provides further evidence that the plain meaning of the statute is clear: Section 1030 asks only whether the accused had authorized access to the computer and information in question. It does not contemplate an inquiry into what an accused otherwise does with properly accessed information.

B. The Legislative History of 18 U.S.C. Section 1030 Clearly Shows that “Exceeding Authorized Access” Does Not Involve an Inquiry into the Purposes for Which the Information is Used

18. The legislative history of Section 1030 leaves no doubt that “exceeding authorized access” is strictly limited to the question of whether the accused who had authorized access to the computer, accessed information that he was not entitled to access. It does not encompass an analysis into the purposes for which information accessed with authorization is ultimately used. Otherwise stated, the section is intended to criminalize intruders who trespass on computer networks, in the sense of circumventing technological restrictions on access. It is not intended to criminalize the acts of those persons who, while authorized to access the information in question, happen to use computers in carrying out an underlying criminal offense.⁵ In 2008, the Congressional Research Service issued a report which analyzed Section 1030 and specifically acknowledged that the statute “outlaws conduct that victimizes computers. It is a computer security law. It protects computers in which there is a federal interest.” Charles Doyle, Cong. Research Service, *Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws* 1 (2008). Just as most modern jurisdictions have trespass laws, intended to protect real property – as opposed to larceny laws protecting the chattel located on that property – Section 1030 was passed to protect computers, not the information located on those computers.

19. Section 1030 was originally enacted in 1984. Act of Oct. 12, 1984, Pub. L. No. 98-473, §§ 2101-2103, 98 Stat. 1837, 2190-92. In that 1984 version, Section 1030(a)(1) punished whoever

⁵ Indeed, this would seem to be a common sense proposition. An act which is carried out through the use of a computer is not more culpable or criminal than one which is carried out without the use of a computer. That is, the alleged disclosure of documents to WikiLeaks through a computer should not carry a greater penalty than the alleged disclosure of paper documents to the same organization. The use of the computer in carrying out the alleged offense should not result in greater legal punishment.

knowingly accesses a computer without authorization, *or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend*, and by means of such conduct obtains information that has been determined by the United States Government . . . to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . . with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation.

Id. § 2102(a), 98 Stat. 2190 (emphasis supplied). In 1986, Congress replaced the phrase “or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend” with the phrase “or exceeds authorized access.” Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2(c), 100 Stat. 1213. In the same Act, Congress added to Section 1030 the definition of “exceeds authorized access” that is presently codified at Section 1030(e)(6). *Id.* § 2(g)(4); *see* 18 U.S.C. § 1030(e)(6).

20. This significant change in language in Section 1030(a)(1) belies any argument that the term “exceeds authorized access” extends to situations where an accused who has authorization to use the computer uses the access for *purposes* to which the authorization does not extend. Clearly, Congress was quite capable of drafting language which would criminalize using a computer or the information contained therein in a way that is inconsistent with the governing terms of use or the computer owner’s interests. The language in the prior statute covered this situation perfectly; it criminalized the scenario where a person “uses the opportunity that such [authorized] access provides for purposes to which such authorization does not extend.” Pub. L. No. 98-473, § 2102, 98 Stat. at 2190; *see Walsh Bishop Assocs., Inc.*, 2012 WL 669069, at *3 (“Further, the legislative purpose and history supports the plain meaning of the statute. Congress enacted [Section 1030] to deter ‘the criminal element from abusing computer technology in future frauds.’ H.R. Rep. No. 98-894, at 4 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3690. As originally enacted, [Section 1030] applied to a person who (1) knowingly accessed without authorization or (2) ‘having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.’ Pub. L. No. 98-473, § 2102, 98 Stat. 2190, 2190-91 (1984). Congress amended the statute by replacing the latter means of access with the phrase ‘exceeds authorized access.’ *See* Pub. L. No. 99-474, § 2, 100 Stat. 1213, 1213 (1986). The stated reason for the amendment was to ‘eliminate coverage for authorized access that aims at purposes to which such authorization does not extend.’ *See* S. Rep. No. 99-432, at 21 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2495 (internal quotation marks omitted). As a result, Congress amended the statute to remove use as a basis for exceeding authorization.”); *Condux Int’l, Inc. v. Haugum*, No. 08-4824 ADM/JSM, 2008 WL 5244818, at *5 (D. Minn. Dec. 15, 2008) (“Had Congress [under Section 1030] intended to target how a person makes use of information, it would have explicitly provided language to that effect.”).

21. In the Senate report on the 1986 amendment of this phrase, Senators Mathias and Leahy commented favorably on the substitution of “exceeds authorized access” for the pre-1986 language of Section 1030:

[The 1986 Amendments] would eliminate coverage for unauthorized access that aims at “purposes to which such authorization does not extend.” This removes from the sweep of the statute one of the murkier grounds of liability, under which a Federal employee’s access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization.

S. Rep. No. 99-432, at 21, *reprinted in* 1986 U.S.C.C.A.N. at 2494-95;⁶ *see also* Aleynikov, 737 F. Supp. 2d at 192-93 n.23 (discussing legislative history behind 1986 amendments to the language of Section 1030); *Shamrock Foods*, 535 F. Supp. 2d at 966 (“[T]he legislative history confirms that [Section 1030] was intended to prohibit electronic trespassing, not the subsequent use or misuse of information.”); *Int’l Ass’n of Machinists & Aerospace Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 499 n.12 (D. Md. 2005) (explaining the purpose of the change in legislative language).

22. Additionally, when Congress amended Section 1030(a)(1) in 1996, it helpfully clarified the interplay between that section and the espionage statutes:

Although there is considerable overlap between 18 U.S.C. [Section] 793(e) and [S]ection 1030(a)(1), as amended by the NII Protection Act, the two statutes would not reach exactly the same conduct. Section 1030(a)(1) would target those persons who deliberately *break into a computer* to obtain properly classified Government secrets then try to peddle those secrets to others, including foreign governments. In other words, unlike existing espionage laws prohibiting the theft and peddling of Government secrets to foreign agents, [S]ection 1030(a)(1) would require proof that the individual knowingly used a computer without authority, or in excess of authority, for the purpose of obtaining classified information. In this sense then, *it is the use of the computer which is being proscribed*, not the unauthorized possession of, access to, or control over the classified information itself.

S. Rep. No. 104-357 (1996) (emphases supplied). As this passage makes clear, a person’s intent in accessing the computer (e.g., to steal government secrets) is entirely distinct from the inquiry of whether that person has authorization to access the computer or information in question (i.e. whether that person is in essence “breaking into” that computer). A purpose to steal government information may be relevant to a prosecution under 18 U.S.C. Section 793(e), which prohibits theft and peddling of government secrets. However, that purpose cannot determine whether a person has “broken into” a computer by accessing it without authority or by accessing information in excess of his authority.

⁶ By way of elaboration, Congress never actually intended to give the Computer Crimes Fraud Act such expansive interpretation. Senators Mathias and Leahy appended their own statement to the Report and explained in more detail the reason for the 1986 amendments. They explained how the original version of the CFAA had been passed in haste, as part of a legislative rider. *See* S. Rep. No. 99-432, at 20-21, *reprinted in* 1986 U.S.C.C.A.N. at 2494. As a result, in 1984, the House had never voted on a series of narrowing amendments, which had been unanimously approved by the Senate. The purpose of the 1986 amendments was to fix the shortcomings of the original version. *See id.* at 20-22.

23. That Congress intended for Section 1030 to criminalize computer crimes, and not the underlying criminal or tortious conduct carried out on the computer, is readily apparent from looking at the full name of the statute – the Computer Fraud and Abuse Act (CFAA). The primary purpose of the CFAA “was to create a cause of action against computer hackers (e.g., electronic trespassers).” *Int’l Ass’n of Machinists & Aerospace Workers*, 390 F. Supp. 2d at 495 (quoting *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp. 2d 817, 820 (E.D. Mich. 2000)) (internal quotations omitted). As the House Report explained, the bill was aimed largely at hackers who “trespass into” computers: “[T]he conduct prohibited is analogous to that of ‘breaking and entering’ rather than using a computer . . . in committing the offense.” H.R. Rep. No. 98-894, at 20 (1984), *reprinted in* 1984 U.S.C.A.N. 3689, 3706. As Professor Orrin Kerr argues:

[T]he available evidence suggests that legislators mostly saw such statutes as doing for computers what trespass and burglary laws did for real property. For example, the House Report on the first federal computer crime legislation passed in 1984 noted that “[S]ection 1030 deals with an ‘unauthorized access’ concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of ‘breaking and entering’ rather than using a computer (similar to the use of a gun) in committing the offense.” Several state statutes incorporated this concept into the titles of their computer crime statutes, labeling the new unauthorized access crimes as crimes of “Computer Trespass.” The legislative histories of computer crime laws also regularly refer to the activity prohibited by unauthorized access statutes as computer trespasses or “breaking into computer systems.”

Orrin S. Kerr, *Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1617-18 (2003) [hereinafter Kerr, *Cybercrime’s Scope*] (footnotes omitted).

24. Thus, the legislative history of both: a) the term “exceeds authorized access” and; b) the CFAA as a whole, clearly reveal what Congress intended when it enacted the statute. It intended that the section would criminalize those who strayed beyond the technical authorization they were given. It did not intend to criminalize those who used a computer for an improper purpose or in contravention of the governing terms of use, even if that use amounted to a criminal offense.

C. Case Law Supports the View that An Accused’s Purpose in Accessing the Computer or the Information is Entirely Irrelevant to Whether an Accused “Exceeded Authorized Access” Under 18 U.S.C. Section 1030(a)(1)

25. A large number of courts have appropriately applied the plain meaning of Section 1030 and thus distinguished between two very distinct scenarios: exceeding authorized *access* and exceeding authorized *use*. See *Nosal III*, 2012 WL 1176119, at *8; *Aleynikov*, 737 F. Supp. 2d at 192; *Zhang*, 2010 WL 4807098, at *3. This interpretation of “exceeds authorized access” has been adopted in the civil context as well. See, e.g., *Walsh Bishop Assocs., Inc.*, 2012 WL

669069, at *2-3; *Xcedex, Inc.*, 2011 WL 2600688, at *4; *Océ N. Am., Inc. v. MCS Servs., Inc.*, 748 F. Supp. 2d 481, 485-87 (D. Md. 2010); *AtPAC, Inc. v. Aptitude Solutions, Inc.*, 730 F. Supp. 2d 1174, 1181 (E.D. Cal. 2010); *Univ. Sports Publ'ns Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 283-85 (S.D.N.Y. 2010); *Lewis-Burke Assocs. LLC v. Widder*, 725 F. Supp. 2d 187, 192-94 (D.D.C. 2010); *Orbit One Commc'ns, Inc.*, 692 F. Supp. 2d at 385-86; *Bell Aerospace Servs., Inc. v. United States Aero Servs., Inc.*, 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010) (“Exceeds authorized access” should not be confused with exceeds authorized use.”); *ReMedPar, Inc. v. Allparts Med., LLC*, 683 F. Supp. 2d 605, 610-13 (M.D. Tenn. 2010); *Bro-Tech Corp. v. Thermax, Inc.*, 651 F. Supp. 2d 378, 406-07 (E.D. Pa. 2009); *Jet One Group, Inc. v. Halcyon Jet Holdings, Inc.*, No. 08-CV-3980 (JS)(ETB), 2009 WL 2524864, at *5-6 (E.D.N.Y. Aug. 14, 2009); *State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309, 315-17 (E.D. Va. 2009); *Condux Int'l, Inc.*, 2008 WL 5244818, at *4-6; *Int'l Ass'n of Machinists & Aerospace Workers*, 390 F. Supp. 2d at 498-99.

26. This proper interpretation was most recently adopted by the en banc Ninth Circuit Court of Appeals in *Nosal III*. In *Nosal III*, employees of the defendant's former employer, using their accounts to access the employer's computer system, provided the defendant with trade secrets and other proprietary information of the employer. 2012 WL 1176119, at *1. The employer placed several limitations on its employees' access of its system, including a restriction on the use or disclosure of all information available on that system, except for legitimate company business. *Id.* at *1 & n.1. The defendant was charged with aiding and abetting the employees' violations of Section 1030(a)(4).⁷ *Id.* at *1. The defendant moved to dismiss the counts of the indictment alleging violations of Section 1030(a)(4), “arguing that the statute targets only hackers, not individuals who access a computer with authorization but then misuse information they obtain by means of such access.” *Id.* The district court ultimately agreed with the defendant's position and granted the motion to dismiss. *Id.*

27. A majority of a panel of three judges of the Ninth Circuit reversed, holding that “an employee ‘exceeds authorized access’ under [Section] 1030 when he or she violates the employer's access restrictions – including use restrictions.” *United States v. Nosal (Nosal I)*, 642 F.3d 781, 785 (9th Cir. 2011), *reh'g en banc granted*, 661 F.3d 1180 (9th Cir. 2011). To support its expansive interpretation, the majority focused on one word in the definition of “exceeds authorized access” provided in Section 1030(e)(6): “so.” See *Nosal I*, 642 F.3d at 785-86. The court reasoned that the word “[s]o” in this context means “in a manner or way that is indicated or suggested.” *Id.* at 785 (quoting *Webster's Third New Int'l Dictionary* 2159 (Philip Babcock Gove, ed. 2002)). In her dissent, Judge Campbell identified two major flaws with the panel opinion: its reliance on the word “so” was misplaced, and its interpretation of the term “exceeds authorized access” rendered at least one provision of Section 1030 unconstitutionally vague. *Id.* at 789-91 (Campbell, J., dissenting).

⁷ Section 1030(a)(4) punishes whoever

knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period[.]

¹⁸ U.S.C. § 1030(a)(4) (emphasis supplied).

28. After granting the defendant's petition for rehearing en banc and withdrawing the panel opinion, *see United States v Nosal (Nosal II)*, 661 F.3d 1180, 1180 (9th Cir. 2011), the en banc Ninth Circuit, in a 9-2 opinion authored by Chief Judge Kozinski, affirmed the district court's dismissal of the Section 1030 counts of the defendant's indictment. *See Nosal III*, 2012 WL 1176119, at *8. The court held that "'exceeds authorized access' in the CFAA is limited to violations of restrictions on access to information, and not restrictions on its use." *Id.* (emphases in original). The *Nosal III* Court found this interpretation of "exceeds authorized access" to be most consistent with the statutory text and structure of the CFAA, as well as the legislative history of that statute.

29. The court first explained why the word "so" in Section 1030(e)(6)'s definition of "exceeds authorized access" could not bear the weight the Government and the panel majority assigned to it:

The government's interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute. This places a great deal of weight on a two-letter word that is essentially a conjunction. If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions – which may well include everyone who uses a computer – we would expect it to use language better suited to that purpose.

Id. at *2. Moreover, "Congress could just as well have included 'so' as a connector or for emphasis." *Id.*

30. The *Nosal III* Court also reasoned that interpreting the phrase "exceeds authorized access" to only proscribe violations of access restrictions, and not violations of use restrictions, would be most consistent with the structure of the CFAA as a whole. *Id.* at *3-4. Because the phrase is used in several different provisions of the CFAA, the court was mindful that its interpretation of the phrase would control each provision of Section 1030 in which the phrase appears. *See id.* at *4. The court was troubled with the effect the Government's interpretation would have on one particular provision of the CFAA:

Subsection 1030(a)(2)(C) requires only that the person who "exceeds authorized access" have "obtain[ed] . . . information from any protected computer." Because "protected computer" is defined as a computer affected by or involved in interstate commerce – effectively all computers with Internet access – the government's interpretation of "exceeds authorized access" makes every violation of a private computer use policy a federal crime.

Id. at *3 (ellipsis and alteration in original). This scenario would pose serious notice and arbitrary enforcement concerns. *See id.* at *3-6 (discussing these concerns); *see also* Part E, *infra* (explaining the *Nosal III* Court's discussion of these concerns).

31. Finally, the *Nosal III* Court determined that its interpretation was most consistent with the CFAA's overarching purpose and legislative history. *Nosal III*, 2012 WL 1176119, at *3. Congress's primary aim in enacting the CFAA was to target computer hacking. *Id.* The court explained how its interpretation of the term "exceeds authorized access" kept this purpose in mind:

[I]t is possible to read both prohibitions as applying to hackers: "[W]ithout authorization" would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and "exceeds authorized access" would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files). This is a perfectly plausible construction of the statutory language that maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate.

Id. (emphases in original). The court went on to note that Congress's replacement of the phrase "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend" with the phrase "exceeds authorized access" further supported its interpretation of that term, and further undermined the Government's proposed interpretation. *Id.* at *3 n.5.

32. The United States District Court for the Southern District of New York reached the same conclusion in *United States v. Aleynikov*. In *Aleynikov*, the defendant, a Goldman Sachs computer programmer copied, compressed, encrypted and transferred hundreds of thousands of lines of Goldman Sachs' source code, which he later gave to his new employer. 737 F. Supp. 2d at 174-75. The defendant was authorized to access the Goldman computer he accessed and to access the source code he accessed, though Goldman Sachs required each computer programmer to sign a confidentiality agreement and limited access to its source code to those employees who have reason to access it. *Id.* at 175, 190-91. The defendant was indicted for unauthorized access and exceeding authorized access under Section 1030(a)(2)(C). *Id.* at 190. The defendant moved to dismiss this count of the indictment, arguing that Section 1030 "does not encompass an employee's misuse or misappropriation of information that the employee has authority to access." *Id.* at 191.

33. The court granted the defendant's motion to dismiss the Section 1030(a)(2)(C) count of the indictment and held that "a person who 'exceeds authorized access' has permission to access the computer, but not the particular information on the computer that is at issue." *Id.* at 191-92. The court explained that:

Section 1030(a)(2)(C) therefore addresses only the unauthorized procurement or alteration of information. The phrase[] . . . "exceeds authorized access" *cannot be read to encompass an individual's misuse or misappropriation of information to which the individual was permitted access. What use an individual makes of the accessed information is utterly distinct from whether the access was authorized in the first place.* The Government's theory that [Section 1030] is violated whenever an individual uses information on a computer in a manner contrary to

the information owner's interest would therefore require a departure from the plain meaning of the statutory text.

Id. at 192 (emphasis supplied). The court further explained that its interpretation was consistent with the statutory text, the overall purpose and structure of Section 1030, and the legislative history of the section. *Id.* at 192-93 & n.23.

34. The Ninth Circuit also reached a similar result in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (2009).⁸ In that case, an employer brought an action against its former employee under Section 1030(g),⁹ alleging that the former employee exceeded authorized access when he emailed documents to himself and his wife "to further his own personal interests, rather than the interests of [his employer]." *Brekka*, 581 F.3d at 1132; *see id.* at 1129-30. The Court rejected the plaintiff's reading of the phrase "exceeds authorized access:"

No language in the CFAA supports LVRC's argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest. Rather, the definition of "exceeds authorized access" in [Section] 1030(e)(6) indicates that Congress did not intend to include such an implicit limitation in the word "authorization." Section 1030(e)(6) provides: "the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6) In other words, for purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations. It is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or "without authorization."

This leads to a sensible interpretation of [Sections] 1030(a)(2) and (4), which gives effect to both the phrase "without authorization" and the phrase "exceeds authorized access": a person who "intentionally accesses a computer without authorization," §§ 1030(a)(2) and (4), accesses a computer without any permission at all, while a person who "exceeds authorized access," *id.*, has permission to access the computer, but accesses information on the computer that the person is not entitled to access.

Id. at 1133. This reasoning was also echoed by the court in *International Association of Machinists & Aerospace Workers*, where the plaintiff argued that the defendant, a union officer, exceeded her authorization to use the union computer when she violated the terms of use to access a membership list with the purpose to send it to a rival union, and not for legitimate union

⁸ Although *Brekka* is a civil case, it involves the interpretation of a criminal statute. As the *Brekka* court itself notes, its interpretation "is equally applicable in the criminal context." 581 F.3d at 1134. With that said, civil cases that use an expansive interpretation of Section 1030 should be viewed with extreme caution. *See* note 10, *infra*.

⁹ 18 U.S.C. Section 1030(g) provides a right of action for private persons injured by computer crimes.

business. 390 F. Supp. 2d at 495-96. The defendant had signed an agreement promising that she would not access union computers “contrary to the policies and procedures of the [union] Constitution.” *Id.* at 498. The court rejected the application of Section 1030, holding that even if the defendant breached a contract, breaking a promise not to use information stored on union computers in a particular way did not mean her access to that information was unauthorized or criminal:

Thus, to the extent that Werner-Masuda may have breached the Registration Agreement by *using* the information obtained for purposes contrary to the policies established by the [union] Constitution, it does not follow, as a matter of law, that she was not authorized to access the information, or that she did so in excess of her authorization in violation of the [Stored Communications Act] or the CFAA . . . Although Plaintiff may characterize it as so, the gravamen of its complaint is not so much that Werner-Masuda improperly accessed the information contained in VLodge, but rather what she did with the information once she obtained it . . . Nor do [the] terms [of the Stored Communications Act and the CFAA] proscribe authorized access for unauthorized or illegitimate purposes.

Id. at 498-99 (emphasis in original). The court captured the issue perfectly when it explained that “the gravamen of [the] complaint is not so much that [the accused] improperly accessed the information . . . but rather what [the accused] did with the information once [the accused] obtained it.” *Id.* at 499. The Government in the instant case has made the same mistake. The gravamen of the offense alleged is that PFC Manning allegedly transmitted classified information to persons not authorized to receive it. It just so happens that a computer was the means by which he is alleged to have done so. This does not, in any circumstances, mean that PFC Manning exceeded authorized access within the meaning of Section 1030.

35. These cases are representative of the host of other cases that have properly interpreted the term “exceeds authorized access” in Section 1030. *See, e.g., Walsh Bishop Assocs., Inc.*, 2012 WL 669069, at *2-3; *Xcedex, Inc.*, 2011 WL 2600688, at *4; *Océ N. Am., Inc.*, 748 F. Supp. 2d at 485-87 (identifying that the phrase “exceeds authorized access” exclusively prohibits access of a computer without authorization, not an employee’s misuse of information that the individual was permitted to access); *AltPac, Inc.*, 730 F. Supp. 2d at 1181 (“[T]he definition of the term ‘exceeds authorized access’ is one that simply examines whether the accessor was entitled to access the information for any purpose.”); *Univ. Sports Publ’ns Co.*, 725 F. Supp. 2d at 283-85; *Lewis-Burke Assocs. LLC*, 725 F. Supp. 2d at 194 (explaining that “[e]xceeds authorized access” should not be confused with exceeds authorized use.” (internal quotations omitted)); *Orbit One Commc’ns, Inc.*, 692 F. Supp. 2d at 385-86; *Bell Aerospace Servs, Inc.*, 690 F. Supp. 2d at 1272 (“‘Exceeds authorized access’ should not be confused with exceeds authorized use.”); *ReMedPar, Inc.*, 683 F. Supp. 2d at 610-13 (recognizing that “exceeds authorized use” is to be construed narrowly, reasoning that the phrase is not intended to extend to situations where the access was authorized but the use was not); *Bro-Tech Corp.*, 651 F. Supp. 2d at 407 (A defendant’s purpose in accessing a computer is irrelevant to whether he or she exceeds authorized access, even if the purpose in doing so is to misuse or misappropriate the information); *Jet One Group, Inc.*, 2009 WL 2524864, at *5-6; *State Analysis, Inc.*, 621 F. Supp. 2d at 317 (recognizing that “exceeds authorization” is explicitly defined as “to access a computer

with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.” (internal quotations omitted)); *Condux Int'l, Inc.*, 2008 WL 5244818, at *4-6; *Shamrock Foods*, 535 F. Supp. 2d 962 (the defendant had an employee account on the computer he used at the company where he was employed, and was permitted to view the specific files he allegedly emailed to himself; the court held that the CFAA did not apply, even though the emailing was for the improper purpose of benefiting himself and a rival company in violation of the defendant’s confidentiality agreement); *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007) (identifying the narrower interpretation of “exceeding authorized access” as “the more reasoned view,” and holding that “a violation for accessing ‘without authorization’ occurs only where initial access is not permitted. And a violation for ‘exceeding authorized access’ occurs where initial access is permitted but the access of certain information is not permitted.”); *Int'l Ass'n of Machinists & Aerospace Workers*, 390 F. Supp. 2d at 498-99.

36. Notwithstanding Congress’s clear and unambiguous definition of “exceeds authorized access” in Section 1030(e)(6), some courts have erroneously held that the purpose for which a computer or information is accessed is somehow relevant to the inquiry of whether the accused exceeded his authorized access.¹⁰ See, e.g., *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010); *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010) (“[T]he concept of ‘exceeds authorized access’ may include exceeding the purposes for which the access is ‘authorized.’ Access to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded.”). These cases are wrongly decided. Neither the *John* Court nor the *Rodriguez* Court offered any explanation – much less any plausible explanation – as to how its interpretation of “exceeds authorized access” could be squared with the plain meaning of Section 1030. As the court stated in *Aleynikov*:

¹⁰ Many of the cases that hold that a user’s purpose in accessing the computer is relevant to a charge under Section 1030 have been decided in the civil context. These civil cases are inapposite and their reasoning should not be extrapolated to the criminal context. In civil cases, the defendant risks having to pay a fine under Section 1030; in criminal cases, the defendant faces the potential for physical confinement. It stands to reason that civil courts will interpret Section 1030 more broadly than criminal courts. This point is clearly made by Professor Kerr:

The second source of the difficulty is that many cases have interpreted “authorization” in the context of civil disputes rather than criminal prosecutions. The difference tends to push courts in the direction of expansive interpretations of new laws. It is one thing to say that a defendant must pay a plaintiff for the harm his action caused; it is quite another to say that a defendant must go to jail for it. Courts are more likely to hold a defendant liable under an ambiguous statute when the stakes involve a business dispute between two competitors than when the government seeks to punish an individual with jail time. As a result, civil precedents tend to adopt broader standards of liability than do criminal precedents. Because many unauthorized access cases have arisen in a civil context with sympathetic facts, courts have adopted broad approaches to authorization that in a criminal context would criminalize a remarkable swath of conduct involving computers.

Kerr, *Cybercrime's Scope*, *supra*, at 1641-42.

[These cases] identify no statutory language that supports interpreting [Section 1030] to reach misuse or misappropriation of information that is lawfully accessed. Instead, they improperly infer that “authorization” is automatically terminated where an individual “exceed[s] the purposes for which access is ‘authorized.’” But “the definition of ‘exceeds authorized access’ in [Section] 1030(e)(6) indicates that Congress did not intend to include such an implicit limitation in the word ‘authorization.’”

737 F. Supp. 2d at 193 (emphasis supplied) (citations omitted).

37. The en banc *Nosal* Court further pointed out that the *Rodriguez* and *John* decisions were the product of the courts’ failure to consider the broader implications of their holdings. The *Nosal III* Court explained that:

These courts looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the statute’s unitary definition of “exceeds authorized access.” They therefore failed to apply the long-standing principle that we must construe ambiguous criminal statutes narrowly so as to avoid “making criminal law in Congress’s stead.”

2012 WL 1176119, at *6 (quoting *United States v. Santos*, 553 U.S. 507, 514 (2008) (plurality opinion)).

38. Finally, neither the defendant in *John* nor the defendant in *Rodriguez* brought to the court’s attention the very significant 1986 amendment to Section 1030’s text replacing the phrase “having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend” with the phrase “exceeds authorized access.” See Brief for Defendant-Appellant, *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (No. 09-15265), 2010 WL 5650308; Reply Brief for Defendant-Appellant, *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (No. 09-15265), 2010 WL 5650310; Brief for Defendant-Appellant, *United States v. John*, 597 F.3d 263 (5th Cir. 2010) (No. 08-10459), 2008 WL 7986381; Reply Brief for Defendant-Appellant, *United States v. John*, 597 F.3d 263 (5th Cir. 2010) (No. 08-10459), 2008 WL 7986383. The Government in each case similarly failed to discuss this crucial piece of legislative history. See Brief for Appellee United States, *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (No. 09-15265), 2010 WL 5650309; Brief for Appellee United States, *United States v. John*, 597 F.3d 263 (5th Cir. 2010) (No. 08-10459), 2008 WL 7986382. Had they done so, the result would likely have been different.

39. The imprudent expansive interpretation of “exceeds authorized access” adopted by the *Rodriguez* and *John* courts should be rejected because it is inconsistent with the plain text of Section 1030 and contrary to congressional intent.

40. As discussed, the plain language of Section 1030(e)(6) in no way indicates that the purposes of an accused in accessing the information or violations of access restrictions can establish that an accused has exceeded authorized access if he has authority to access the computer and to access the information. See 18 U.S.C. § 1030(e)(6) (“[T]he term ‘exceeds authorized access’

means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter[.]”). If the accused has authorization to access the computer and obtains information that the accused has authorization to obtain, the accused cannot, under the plain language of Section 1030(e)(6), be held to have exceeded his authorized access. Interpreting “exceeds authorized access” to include an accused’s misuse of information or violation of access restrictions is inconsistent with the plain language of Section 1030(e)(6) and with the legislative history of Section 1030.

41. Even if a court could “get past” the problems with statutory interpretation, there is another serious infirmity in the interpretation advanced by courts that ascribe an expansive interpretation of Section 1030. These courts require an analysis into an accused’s subjective intent at the time he accessed the relevant information in order to determine whether he exceeded his authorized access. In other words, “exceeding authorized access” becomes a shifting standard depending on a person’s intent at the time they accessed the information. For instance, consider a corporate lawyer who uses his employer’s computer to search for information on what deals the firm is working on. He has full access to the firm’s computers and full authority to access and read client files. As he is perusing the files, he discovers information that a corporate client has overstated its revenues and would be issuing a public statement to that effect the subsequent week. He owns shares of that company and, based on the information he has acquired, decides a few days later to sell his shares. The law firm’s terms of use specify that lawyers may not use firm information for their personal financial gain. Has the lawyer “exceeded authorized access” because he violated the terms of use? Certainly, the lawyer may be guilty of insider trading or may have violated ethical canons – but he did not exceed authorized access under the expansive (and incorrect) interpretation of Section 1030 because, at the time he accessed the information, he had no intent to use the information for a purpose contrary to the terms of use. If, however, the lawyer went looking for information on the computer on the particular client with the intention of using it for his own purposes, under the interpretation offered by *Rodriguez and John*, the lawyer would be exceeding authorized access because he exceeded the firm’s terms of use. Thus, the very same act – looking at the financial information of a corporate client – would be punishable under Section 1030 in some cases, but not in others.¹¹

42. This variable standard cannot be what Congress intended. Either a person has exceeded authorized access (in that they accessed information that they did not have permission to access) or they did not. The determination cannot be a nebulous inquiry into an accused’s state of mind at the time he accessed material that he had authorization to access. See *Aleynikov*, 737 F. Supp. 2d at 194 (“The interpretation of [Section 1030] adopted in this line of cases would require an analysis of an individual’s subjective intent in accessing a computer system, whereas the text of

¹¹ Indeed, the en banc Ninth Circuit raised this very possibility in the *Nosal* rehearing in reference to a hypothetical defendant who sold security information to a hostile power. One judge asked, “Does the employee violate the Act if the employee has security clearance to be into the database but the government has said, ‘You may access this database as long as you don’t sell it to a hostile power.’ And somebody takes the information to which they are authorized to be there by virtue of their security clearance but then takes it and sells it to a hostile power?” Oral Argument at 14:14, *United States v. Nosal*, No. 10-10038 (9th Cir. Dec. 15, 2011) (en banc), available at http://www.ca9.uscourts.gov/media/view_subpage.php?pk_id=0000008546. The Government’s position was that this would constitute “exceeding authorized access” under Section 1030 provided that the defendant had a prohibited purpose at the time of the access. *Id.* at 14:40. However, the Government conceded that if the defendant obtained the information and decided to sell it later, this would not violate Section 1030. *Id.* at 15:14.

[Section 1030] calls for only an objective analysis of whether an individual had sufficient 'authorization.' While a confidentiality agreement or other policies or obligations owed to an employer may prohibit misuse of a company's internal computer system or misappropriation of confidential information therein, the plain text of [Section 1030] does not.”).

D. The Rule of Lenity Requires That “Exceeds Authorized Access” Be Read in Its Narrow Sense

43. The Defense submits that the meaning of “exceeds authorized access” is abundantly clear, both by its plain meaning and through an analysis of the legislative history. The Government, however, submits that the accused’s purpose in accessing the information in question should be grafted onto Section 1030. Thus, the Government posits that an individual can exceed authorized access by accessing information with a subjective purpose that is inconsistent with the governing use policy or the computer owner’s interests. To the extent that there are two possible interpretations of a statute – one broad and one narrow – courts should apply the rule of lenity and adopt the narrow interpretation.

44. It is well established that “ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity.” *United States v. Carr*, 513 F.3d 1164, 1168 (9th Cir. 2008) (quoting *Rewis v. United States*, 401 U.S. 808, 812 (1971)). The Supreme Court has long warned against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants. See *Santos*, 553 U.S. at 514 (2008) (citing *United States v. Bass*, 404 U.S. 336, 347-49 (1971); *McBoyle v. United States*, 283 U.S. 25, 27 (1931); *United States v. Gradwell*, 243 U.S. 476, 485 (1917)). “This venerable rule . . . vindicates the fundamental principle that no citizen should be held accountable for a violation of a statute whose commands are uncertain, or subjected to punishment that is not clearly prescribed.” *Id.* Therefore, “[t]he rule of lenity, which is rooted in considerations of notice, requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government.” *United States v. Romm*, 455 F.3d 990, 1001 (9th Cir. 2006).

45. Military courts have accepted the rule of lenity when construing ambiguous criminal statutes. See *United States v. Schelin*, 15 M.J. 218, 220 (C.M.A. 1983); *United States v. Cartwright*, 13 M.J. 174, 176 & n.4 (C.M.A. 1982); *Inthavong*, 48 M.J. at 630 (“This policy of lenity means that [courts] will not interpret a federal criminal statute so as to increase the penalty that it places on an individual when such an interpretation can be based on *no more than a guess* as to what Congress intended.” *Ladner v. United States*, 358 U.S. 169, 178, 79 S.Ct. 209, 214, 3 L.Ed.2d 199 (1958) (emphasis added)); *United States v. Ferguson*, 40 M.J. 823, 830 (N.M.C.M.R. 1994) (“It is an ancient rule of statutory construction that penal statutes should be strictly construed against the government . . . and in favor of the persons on whom penalties are sought to be imposed.” Sutherland Stat Const § 59.03 (5th Ed). A corollary to the rule of strict construction is the ‘rule of lenity’ whereby ambiguities in penal statutes are resolved in favor of lenity. *Id.* Statutes that declare conduct criminal or laws that expressly define or limit punishments for any offense are classified as penal. *Id.* at § 59.02. The UCMJ is a penal statute. Rule for Courts-Martial (R.C.M.) 201, MCM, United States, 1984. With an eye to *Levy*, we conclude the UCMJ is generally subject to the rule of strict construction and the “rule of lenity.” See *United States v. Schelin*, 15 M.J. 218 (C.M.A.1983)).”.

46. Thus, under the rule of lenity, this Court should adopt the narrow meaning of “exceeds authorized access.” That is, one exceeds authorized access when one bypasses technical, computer-based restrictions to access information on the computer than one is not entitled to access. This is exactly what the Ninth Circuit held in *Nosal III*:

If Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly. The rule of lenity requires “penal laws . . . to be construed strictly.” *United States v. Wiltberger*, 18 U.S. (5 Wheat.) 76, 95, 5 L.Ed. 37 (1820). “[W]hen choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite.” *Jones v. United States*, 529 U.S. [848.] 858, 120 S.Ct. 1904 [(2000)] (internal quotation marks and citation omitted).

The rule of lenity not only ensures that citizens will have fair notice of the criminal laws, but also that Congress will have fair notice of what conduct its laws criminalize. We construe criminal statutes narrowly so that Congress will not unintentionally turn ordinary citizens into criminals. “[B]ecause of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity.” *United States v. Bass*, 404 U.S. 336, 348, 92 S.Ct. 515, 30 L.Ed.2d 488 (1971). “If there is any doubt about whether Congress intended [the CFAA] to prohibit the conduct in which [Nosal] engaged, then ‘we must choose the interpretation least likely to impose penalties unintended by Congress.’” *United States v. Cabacang*, 332 F.3d 622, 635 n.22 (9th Cir.2003) (quoting *United States v. Arzate-Nunez*, 18 F.3d 730, 736 (9th Cir.1994)).

This narrower interpretation is also a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking – the circumvention of technological access barriers – not misappropriation of trade secrets – a subject Congress has dealt with elsewhere Therefore, we hold that “exceeds authorized access” in the CFAA is limited to violations of restrictions on access to information, and not restrictions on its use.

2012 WL 1176119, at *7-8 (emphases in original). Applying the rule of lenity and what the Defense submits is the proper understanding of “exceeds authorized access,” the Government has failed to state a claim.

E. An Expansive Reading of “Exceeds Authorized Access” Is Unconstitutionally Vague and Would Lead to Absurd Results

47. An expansive interpretation of “exceeds authorized access” that would criminalize persons for violating terms of authorized use puts at least one provision of Section 1030 in constitutional jeopardy. In *Nosal I*, the defendant argued to the three judge panel of the Ninth Circuit that the Government’s interpretation would “make criminals out of millions of employees who might use

their computers for personal use, for example, to access their personal email accounts or to check the latest college basketball scores.” 642 F.3d at 788. The panel majority rejected this contention, concluding that because Section 1030(a)(4) requires an intent to defraud and an action that furthers the fraud, the defendant’s “Orwellian” fear was unfounded. *Id.* at 788-89.

48. The en banc Ninth Circuit, however, was not so dismissive. After all, the term “exceeds authorized access” is included in both Section 1030(a)(4) – the provision at issue in *Nosal* – and Section 1030(a)(2)(C). See 18 U.S.C. § 1030(a)(2)(C), (4); *Nosal III*, 2012 WL 1176119, at *3. Thus, an interpretation of “exceeds authorized access” for Section 1030(a)(4) purposes is equally applicable to Section 1030(a)(2)(C). *Nosal III*, 2012 WL 1176119, at *4. Section 1030(a)(2)(C) does not require an intent to defraud like Section 1030(a)(4) does. See *id.* at *3-4. Instead, a person is guilty of a violation of Section 1030(a)(2)(C) when that person “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer,” 18 U.S.C. § 1030(a)(2)(C), where the term “protected computer” includes a computer connected to the internet. See *Nosal*, 2012 WL 1176119, at *3-4. Therefore, under “the government’s proposed interpretation, millions of unsuspecting individuals would find that they are engaging in criminal conduct.” *Id.* at *4. The court colorfully elaborated:

Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer-use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes. Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes.

Id.

49. The *Nosal III* Court found this situation intolerable for two reasons, both tied to the void-for-vagueness doctrine. First, the Government’s interpretation posed serious notice concerns. See *id.* Second, it would “invite arbitrary and discriminatory enforcement.” *Id.*

50. The court remarked that “[s]ignificant notice problems arise if we allow criminal liability to turn on the vagaries of private policies that are lengthy, opaque, subject to change and seldom read.” *Id.* The use of countless websites is governed by a series of private agreements and policies. *Id.* at *5. The prevalence of these agreements and policies is rivaled only by their obscurity to the average person; “most people are only dimly aware of [them] and virtually no one reads or understands [them].” *Id.* If the scant notice of their existence wasn’t troublesome enough, “website owners retain the right to change the terms at any time and without notice. Accordingly, behavior that wasn’t criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever.” *Id.* at *6 (citation and parenthetical omitted).¹²

¹² The fact that these notice concerns may not be as apparent in this case should be irrelevant to this Court’s interpretation of the term “exceeds authorized access.” As the en banc *Nosal* Court noted, the interpretation given to the term “exceeds authorized access” is applicable to all provisions of Section 1030 that use some variant of that term. See *Nosal III*, 2012 WL 1176119, at *4 (“Congress obviously meant ‘exceeds authorized access’ to have the

51. In addition to these substantial notice concerns, the *Nosal III* Court also anticipated that the Government's interpretation would lead to arbitrary and discriminatory enforcement. See *id.* at *4, *6. The Government's assurances of prosecutorial restraint did not satisfy the court:

The government assures us that, whatever the scope of the CFAA, it won't prosecute minor violations. But we shouldn't have to live at the mercy of our local prosecutor. Cf. *United States v. Stevens*, --- U.S. ---, 130 S.Ct. 1577, 1591 (2010) ("We would not uphold an unconstitutional statute merely because the Government promised to use it responsibly."). And it's not clear we *can* trust the government when a tempting target comes along. Take the case of the mom who posed as a 17-year-old boy and cyber-bullied her daughter's classmate. The Justice Department prosecuted her under 18 U.S.C. § 1030(a)(2)(C) for violating MySpace's terms of service, which prohibited lying about identifying information, including age. See *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). Lying on social media websites is common: People shave years off their age, add inches to their height and drop pounds from their weight. The difference between puffery and prosecution may depend on whether you happen to be someone an AUSA has reason to go after.

Id. at *6 (emphasis in original).

52. Indeed, as the en banc Ninth Circuit indicated, the "Orwellian situation" that was so casually dismissed by the *Nosal I* panel majority actually came to fruition in *Drew*. In that case, the adult defendant created a false MySpace profile of a teenage boy, posted a picture of a teenage boy to that profile without the boy's consent, used that profile to befriend a teenage girl, and eventually used that profile to tell that teenage girl that "the world would be a better place without her in it." *Drew*, 259 F.R.D. at 452. The teenage girl took her own life later that day, and the defendant was soon indicted for felony violations of Section 1030(a)(2)(C) and (c)(2)(B)(ii). *Id.* The defendant was alleged to have exceeded her authorized access to MySpace.com because her act of creating the false profile and the posting of a picture of a teenage boy without the boy's consent violated MySpace's terms of service. *Id.* The jury acquitted the defendant of the felony violations but convicted her on misdemeanor violations of Section 1030(a)(2)(C). *Id.* at 453. The defendant then filed a motion for judgment of acquittal, contending that the violation of the terms of service of an internet provider cannot constitute exceeding authorized access under Section 1030 and, if it did, Section 1030 was unconstitutionally vague. *Id.* at 451.

53. The United States District Court for the Central District of California granted the defendant's motion, concluding that Section 1030(a)(2)(C), as interpreted by the court and as

same meaning throughout [S]ection 1030. We must therefore consider how the interpretation we adopt will operate wherever in that section the phrase appears."). Therefore, it is no answer to the constitutional concerns raised by the expansive interpretation of the term "exceeds authorized access" to say that no notice concerns are present in this case. Indeed, the *Nosal* panel majority put forth this flawed, myopic rationale, see *Nosal I*, 642 F.3d at 788-89, and that rationale was soundly rejected by the en banc *Nosal* Court, see *Nosal III*, 2012 WL 1176119, at *3-4. The *Rodriguez* and *John* Courts made the same mistake. See *id.* at *6. Accordingly, in choosing the appropriate interpretation of the term "exceeds authorized access" this Court must consider how the chosen interpretation will affect the other provisions of Section 1030. See *id.* at *4.

applied to the defendant's conduct, was unconstitutionally vague. *Id.* at 464-67. First, the court determined that, as it had interpreted Section 1030, the statute presented serious notice problems: "[T]he language of [S]ection 1030(a)(2)(C) does not explicitly state (nor does it implicitly suggest) that [Section 1030] has 'criminalized breaches of contract' in the context of website terms of service." *Id.* at 464. Second, the court explained that under Section 1030(a)(2)(C)'s "standardless sweep" . . . federal law enforcement entities would be improperly free 'to pursue their personal predilections'" in selecting which violations to prosecute and which to let go unpunished. *Id.* at 467 (quoting *Kolender v. Lawson*, 461 U.S. 352, 358 (1983)). Accordingly, the court concluded that its broad interpretation of "exceeds authorized access" rendered Section 1030(a)(2)(C) unconstitutionally vague as applied to the defendant's conduct. *Id.* at 464, 467.

54. Under the Government's interpretation in this case, if an accused violates the governing terms of use, he is guilty of a federal offense under Section 1030. As described above, this interpretation raises serious constitutional concerns of vagueness – concerns which can be readily avoided by interpreting the phrase "exceeds authorized access" according to its plain meaning.

F. Academic Commentary Supports the View that "Exceeds Authorized Access" Under Section 1030 Must be Interpreted Narrowly

55. Professor Orin Kerr, one of the country's foremost experts in the area of computer crimes and cyber law, has argued in two separate articles that the term "exceeding authorized access" should not be interpreted so as to allow for an inquiry into whether the accused has violated the computer owner's terms of use. Rather, Section 1030 should only capture whether the user bypassed technical restrictions so as to access information that he was not entitled to access. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1572 (2010) [hereinafter Kerr, *Vagueness Challenges*]; Kerr, *Cybercrime's Scope*, *supra*, at 1649.

56. Kerr notes that several courts have correctly recognized that "an employee who is authorized to access an employer's computer is, well, authorized to use the employer's computer." Kerr, *Vagueness Challenges*, *supra*, at 1584. Under this interpretation, courts have properly held that misuse of an employer's computer in no way renders the access unauthorized; in fact, the misuse is entirely irrelevant to the "exceeds authorized access" inquiry. *See id.* For Kerr, when access is without authorization or exceeds authorized access must be limited "to access that circumvents restrictions by code." Kerr, *Cybercrime's Scope*, *supra*, at 1649. Kerr has explained this code-based approach as follows:

When a user circumvents regulation by code, she tricks the computer into giving her greater privileges than she is entitled to receive. This normally can occur in two ways. First, a user can enter the username and password of another user with greater privileges . . . Second, a user can exploit a design flaw in software that leads the software to grant the user greater privileges[.]

Id. (footnote omitted).

57. He views this narrow interpretation as not only correct, but absolutely essential to the CFAA's vitality: "Only a narrow construction of the statute can save its constitutionality." Kerr, *Vagueness Challenges*, *supra*, at 1572. Kerr reasons that a narrow construction is necessary because a more expansive interpretation, like the one adopted by the *John* and *Rodriguez* courts, would likely render Section 1030 both substantially overbroad and unconstitutionally vague. See Kerr, *Cybercrime's Scope*, *supra*, at 1658-59.

58. If "exceeds authorized access" is interpreted to cover a person's violations of a website's terms of service or a person's misuse or misappropriation of information that the person was authorized to access in the first place, the overbreadth doctrine is implicated because Section 1030 would in effect be "granting computer owners the power to criminalize speech, and even mere thoughts." *Id.* at 1658. Kerr provides the following example to illustrate this point:

[A] pro-life owner of a computer network could insert a paragraph in the Terms of Use agreement allowing only those who express pro-life opinions (or even only those who are pro-life) to use the network. Expressing pro-choice viewpoints would violate the Terms of Use, making the access "without authorization" or "exceeding authorized access" and triggering criminal liability.

Id. at 1658-59. The First Amendment would be seriously offended if the CFAA gave a computer owner the power to "harness the criminal law at his discretion" in this manner. *Id.* at 1658

59. Even more problematic, Kerr argues, an expansive interpretation of "exceeds authorized access" would pose serious vagueness concerns. See Kerr, *Vagueness Challenges*, *supra*, at 1562, 1572; Kerr, *Cybercrime's Scope*, *supra*, at 1659. "The CFAA has become so broad, and computers so common, that expansive or uncertain interpretations of unauthorized access . . . would either provide insufficient notice of what is prohibited or fail to provide guidelines for law enforcement in violation of the constitutional requirement of Due Process[.]" Kerr, *Vagueness Challenges*, *supra*, at 1562. If a website's terms of service can limit a user's access, as the court held in *Drew*, the notice problems are readily apparent:

Few users read the terms of service or terms of use of any of the computers they access, much less all of them, and many restrictions feature ambiguous terms that can be quite difficult to interpret. It is difficult, if not impossible, for a typical user to know for sure whether he is in compliance with all of the contractual restrictions regulating each of the computers he has accessed at any given time. Under the broad contractual theory of authorization, however, any violation of the terms of service or terms of use of any computer a person accesses violates the statutory prohibition on unauthorized access.

Kerr, *Cybercrime's Scope*, *supra*, at 1659. The notice problems are just as serious under the expansive interpretation adopted in *John* and *Rodriguez* where an employee's use of information for personal reasons, or contrary to the interests of the employer, can be considered exceeding authorized access:

[W]e need to recognize that many employees routinely use protected computers in the course of their day for a tremendously wide range of functions. Employee use of computers tracks employee attention spans. Attention wanders, and our computer use wanders with it. We think, therefore we Google. As a result, it is rare, if not inconceivable, for every keystroke to be clearly and strictly in the course of furthering an employment relationship. The best employee in a larger company might spend thirty minutes writing up a report, and then spend one minute checking personal e-mail and twenty seconds to check the weather to see if the baseball game after work might be rained out. He might then spend ten more minutes working on the report followed by two minutes to check the online news. Over the course of the day, he might use the computer for primarily personal reasons dozens or even hundreds of times.

Kerr, *Vagueness Challenges, supra*, at 1585.

60. For these reasons, Kerr concludes that “[t]he acts of violating [a website’s terms of service] and acting contrary to an employer’s interest, without more, should not constitute either an access without authorization or exceeding an authorized access.” *Id.* at 1572. Such an interpretation would “create a remarkably broad criminal prohibition that has no connection to the rationales of criminal punishment.” Kerr, *Cybercrime’s Scope, supra*, at 1663.

61. Kerr is by no means alone in advocating the necessity of a narrow interpretation of “exceeds authorized access.” Indeed, several other commentators have echoed the same refrain. *See, e.g.,* Thomas E. Booms, Note, *Hacking Into Federal Court: Employee “Authorization” Under the Computer Fraud and Abuse Act*, 13 Vand. J. Ent. & Tech. L. 543, 570 (2011) (advocating a narrow interpretation because “an employee who has permission to access an employer’s computer is authorized to use that computer. It should be irrelevant what the employee does on the computer, because the statute emphasizes access to the computer, not its use. This interpretation is not only supported by the plain meaning of the statute, the CFAA’s legislative history, and the rule of lenity, but also allows for a consistent and predictable application of the statute.” (footnote omitted)); *id.* at 571 (providing the following analogous example: “If a person is invited into someone’s home and steals jewelry while inside, the person has committed a crime – but not burglary – because he has not broken into the home. The fact that the person committed a crime while inside the home does not change the fact that he was given permission to enter.”); Garrett D. Urban, Note, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 Wm. & Mary L. Rev. 1369, 1407 (2011) (“A code-based approach [like the one advocated by Kerr] to the amended CFAA would limit expansive liability while still allowing for changes in technology”); Greg Pollaro, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 2010 Duke L. & Tech. Rev. 12, ¶ 23 (2010), available at <http://dltr.law.duke.edu/2010/08/26/disloyal-computer-use-and-the-computer-fraud-and-abuse-act-narrowing-the-scope/> (“A narrow definition . . . has the dual benefit of providing a clearer standard and being in accord with the initial spirit and purpose of the CFAA.”).

62. Therefore, academic commentary provides even further support for the position that the term “exceeds authorized access” should be interpreted narrowly to only cover situations where a

person accesses information that the person is not authorized to access, regardless of the purposes behind the access.

CONCLUSION

63. The Government in this case has not alleged that PFC Manning “exceeded authorized access” within the proper meaning of Section 1030(a)(1). PFC Manning had access to the relevant SIPRNET computers and was authorized to access every piece of information that he allegedly accessed on the SIPRNET. As such, because the Government has failed to allege that PFC Manning’s conduct exceeded his authorized access under Section 1030(a)(1), the specifications alleging violations of Section 1030(a)(1) must be dismissed.

64. Wherefore, in light of the foregoing, the Defense requests this Court dismiss Specifications 13 and 14 of Charge II because the Government has failed to allege that PFC Manning’s alleged conduct exceeded authorized access within the meaning of Section 1030(a)(1).

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211)

GOVERNMENT RESPONSE TO
DEFENSE MOTION TO DISMISS
SPECIFICATIONS 13 AND 14
OF CHARGE II FOR FAILURE
TO STATE AN OFFENSE

24 May 2012

RELIEF SOUGHT

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny the defense motion to dismiss Specifications 13 and 14 of Charge II for failure to state an offense.

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the defense has the burden of persuasion on any factual issue the resolution of which is necessary to decide the motion. *Manual for Courts-Martial (MCM), United States*, Rule for Courts-Martial (RCM) 905(c)(2) (2008). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

FACTS

The United States stipulates to the facts as set forth in the defense motion. The United States adds the following facts:

While deployed, the accused used two different Secret Internet Protocol Router Network (SIPRNET) computers: (1) a SIPRNET computer with the internet protocol (IP) address of 22.225.41.22; and (2) a SIPRNET computer with the IP address of 22.225.41.40. *See* Enclosure 1 at 126-27, 133. Before logging on to each computer with a username and password, the accused was presented with a warning banner. *See id.* at 134-35. The accused was required to click "OK" after being warned of the following:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC, monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private,

are subject to routine monitoring, interception and search, and may be disclosed or used for any USG authorized purpose. This IS includes security measures (e.g. authentication and access controls) to protect USG-interests—not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content [sic] of privileged [sic] communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement or details.

See id.; Enclosure 2.

During the Article 32 Investigation, the United States proceeded under the theory that because the accused's access to SIPRNET computers was governed by a purpose-based limitation or restriction, the accused exceeded authorized access when he accessed those classified government computers for an unauthorized or expressly forbidden purpose. *See* Enclosure 3. The purpose-based restriction was apparent in the first sentence of the warning banner, which notified the accused that he was "accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only." Enclosure 2; *see* Enclosure 1 at 134-35.

The accused and members of his unit were also required to sign a user agreement or acceptable use policy (AUP) prior to being granted access and a user network account (username and password) for the SIPRNET while deployed. *See* Enclosure 5. The Army's sample AUP states that "[a]ccess to this/these network(s) is for official use and authorized purposes...." *See* Enclosure 6 at 62. The purpose of an AUP is to obtain explicit acknowledgments from individuals on their responsibilities and limitations in using government information systems. *See id.* at 61.

Net-Centric Diplomacy

In response to the attacks of September 11th, Congress tasked the Office of the Director of National Intelligence to find a way to get key government agencies (e.g. Department of Defense (DOD) and Department of State (DOS)) to share information rapidly. *See* Enclosure 4. The Net-Centric Diplomacy Database (NCD), financed by DOD, was developed to provide a full range of diplomatic reporting ("diplomatic cables") to any individual with access to the DOD-controlled SIPRNET. *See id.* at 2. Diplomatic cables were routed to the NCD database or server, and thus made available to individuals with access to the SIPRNET, when the cable was assigned the code "SIPDIS" or "SIPR distribution." *See id.* at 3. In order for a SIPRNET user to access a diplomatic cable, the user must navigate through the SIPRNET to the NCD website (<http://ncd.state.sgov.gov>), and search the website for the desired cable.

INSTRUCTIONS FOR PREPARING AND ARRANGING RECORD OF TRIAL

USE OF FORM - Use this form and MCM, 1984, Appendix 14, will be used by the trial counsel and the reporter as a guide to the preparation of the record of trial in general and special court-martial cases in which a verbatim record is prepared. Air Force uses this form and departmental instructions as a guide to the preparation of the record of trial in general and special court-martial cases in which a summarized record is authorized.

Army and Navy use DD Form 491 for records of trial in general and special court-martial cases in which a summarized record is authorized. Inapplicable words of the printed text will be deleted.

COPIES - See MCM, 1984, RCM 1103(g). The convening authority may direct the preparation of additional copies.

ARRANGEMENT - When forwarded to the appropriate Judge Advocate General or for judge advocate review pursuant to Article 64(a), the record will be arranged and bound with allied papers in the sequence indicated below. Trial counsel is responsible for arranging the record as indicated, except that items 6, 7, and 15e will be inserted by the convening or reviewing authority, as appropriate, and items 10 and 14 will be inserted by either trial counsel or the convening or reviewing authority, whichever has custody of them.

1. Front cover and inside front cover (chronology sheet) of DD Form 490.

2. Judge advocate's review pursuant to Article 64(a), if any.

3. Request of accused for appellate defense counsel, or waiver/withdrawal of appellate rights, if applicable.

4. Briefs of counsel submitted after trial, if any (Article 38(c)).

5. DD Form 494, "Court-Martial Data Sheet."

6. Court-martial orders promulgating the result of trial as to each accused, in 10 copies when the record is verbatim and in 4 copies when it is summarized.

7. When required, signed recommendation of staff judge advocate or legal officer, in duplicate, together with all clemency papers, including clemency recommendations by court members.

8. Matters submitted by the accused pursuant to Article 60 (MCM, 1984, RCM 1105).

9. DD Form 458, "Charge Sheet" (unless included at the point of arraignment in the record).

10. Congressional inquiries and replies, if any.

11. DD Form 457, "Investigating Officer's Report," pursuant to Article 32, if such investigation was conducted, followed by any other papers which accompanied the charges when referred for trial, unless included in the record of trial proper.

12. Advice of staff judge advocate or legal officer, when prepared pursuant to Article 34 or otherwise.

13. Requests by counsel and action of the convening authority taken thereon (e.g., requests concerning delay, witnesses and depositions).

14. Records of former trials.

15. Record of trial in the following order:

a. Errata sheet, if any.

b. Index sheet with reverse side containing receipt of accused or defense counsel for copy of record or certificate in lieu of receipt.

c. Record of proceedings in court, including Article 39(a) sessions, if any.

d. Authentication sheet, followed by certificate of correction, if any.

e. Action of convening authority and, if appropriate, action of officer exercising general court-martial jurisdiction.

f. Exhibits admitted in evidence.

g. Exhibits not received in evidence. The page of the record of trial where each exhibit was offered and rejected will be noted on the front of each exhibit.

h. Appellate exhibits, such as proposed instructions, written offers of proof or preliminary evidence (real or documentary), and briefs of counsel submitted at trial.